ZyWALL 110/310/1100 Series

VPN Firewall

Version 3.10
Edition 2, 02/2013

User's Guide

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Copyright © 2013 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the ZyWALL and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.

- CLI Reference Guide

  The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the ZyWALL.

Note: It is recommended you use the Web Configurator to configure the ZyWALL.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

Chapter 1
Introduction 17

1.1 Overview 17
1.2 Management Overview 19
1.3 Web Configurator 20
1.3.1 Web Configurator Access 20
1.3.2 Web Configurator Screens Overview 21
1.3.3 Navigation Panel 25
1.3.4 Tables and Lists 28

Chapter 2
Installation Setup Wizard 33

2.1 Installation Setup Wizard Screens 33
2.1.1 Internet Access Setup - WAN Interface 33
2.1.2 Internet Access: Ethernet 34
2.1.3 Internet Access: PPPoE 34
2.1.4 Internet Access: PPTP 35
2.1.5 ISP Parameters 35
2.1.6 Internet Access - Finish 36

Chapter 3
Hardware Introduction 37

3.1 Default Zones, Interfaces, and Ports 37
3.2 Stopping the ZyWALL 38
3.3 Rack-mounting 38
3.4 Wall-mounting 39
3.5 Front Panel LEDs 39
3.5.1 Rear Panels 41

Chapter 4
Quick Setup Wizards 43

4.1 Quick Setup Overview 43
4.2 WAN Interface Quick Setup 43
4.2.1 Choose an Ethernet Interface 44
4.2.2 Select WAN Type 44
4.2.3 Configure WAN Settings 45
4.2.4 WAN and ISP Connection Settings 45
4.2.5 Quick Setup Interface Wizard: Summary 47
4.3 VPN Setup Wizard 48
4.3.1 Welcome 48
4.3.2 VPN Setup Wizard: Wizard Type 49
4.3.3 VPN Express Wizard - Scenario 50
4.3.4 VPN Express Wizard - Configuration 51

4.3.5 VPN Express Wizard - Summary 51
4.3.6 VPN Express Wizard - Finish 52
4.3.7 VPN Advanced Wizard - Scenario 53
4.3.8 VPN Advanced Wizard - Phase 1 Settings 54
4.3.9 VPN Advanced Wizard - Phase 2 56
4.3.10 VPN Advanced Wizard - Summary 57
4.3.11 VPN Advanced Wizard - Finish 57
4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type 58
4.4.1 Configuration Provisioning Express Wizard - VPN Settings 59
4.4.2 Configuration Provisioning VPN Express Wizard - Configuration 60
4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary 61
4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish 62
4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario 63
4.4.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings 64
4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2 65
4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary 66
4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish 66

Chapter 5
Dashboard 69

5.1 Overview 69
5.1.1 What You Can Do in this Chapter 69
5.2 The Dashboard Screen 69
5.2.1 The CPU Usage Screen 74
5.2.2 The Memory Usage Screen 75
5.2.3 The Active Sessions Screen 75
5.2.4 The VPN Status Screen 76
5.2.5 The DHCP Table Screen 77
5.2.6 The Number of Login Users Screen 78

Chapter 6
Monitor 79

6.1 Overview 79
6.1.1 What You Can Do in this Chapter 79
6.2 The Port Statistics Screen 80
6.2.1 The Port Statistics Graph Screen 81
6.3 Interface Status Screen 82
6.4 The Traffic Statistics Screen 86
6.5 The Session Monitor Screen 89
6.6 The DDNS Status Screen 91
6.7 IP/MAC Binding Monitor 91
6.8 The Login Users Screen 92
6.9 Cellular Status Screen 93

6.9.1 More Information 95
6.10 USB Storage Screen 96
6.11 The IPSec Monitor Screen 97
6.11.1 Regular Expressions in Searching IPSec SAs 98
6.12 The SSL Connection Monitor Screen 99
6.13 The L2TP over IPSec Session Monitor Screen 99
6.14 Log Screen 100

Chapter 7
Interfaces 103

7.1 Interface Overview 103
7.1.1 What You Can Do in this Chapter 103
7.1.2 What You Need to Know 103
7.1.3 What You Need to Do First 108
7.2 Port Role Screen 108
7.3 Ethernet Summary Screen 109
7.3.1 Ethernet Edit 110
7.3.2 Object References 122
7.3.3 Add/Edit DHCPv6 Request/Release Options 123
7.3.4 Add/Edit DHCP Extended Options 124
7.4 PPP Interfaces 125
7.4.1 PPP Interface Summary 126
7.4.2 PPP Interface Add or Edit 127
7.5 Cellular Configuration Screen (3G) 132
7.5.1 Cellular Add/Edit Screen 134
7.6 Tunnel Interfaces 140
7.6.1 Configuring a Tunnel 142
7.6.2 Tunnel Add or Edit Screen 143
7.7 VLAN Interfaces 147
7.7.1 VLAN Summary Screen 148
7.7.2 VLAN Add/Edit 150
7.8 Bridge Interfaces 159
7.8.1 Bridge Summary 160
7.8.2 Bridge Add/Edit 162
7.9 Virtual Interfaces 170
7.9.1 Virtual Interfaces Add/Edit 171
7.10 Interface Technical Reference 172

Chapter 8
Trunk 177

8.1 Overview 177
8.1.1 What You Can Do in this Chapter 177
8.1.2 What You Need to Know 177

8.2 The Trunk Summary Screen 180
8.2.1 Configuring a User-Defined Trunk 181
8.2.2 Configuring the System Default Trunk 183

Chapter 9
Policy and Static Routes 187

9.1 Policy and Static Routes Overview 187
9.1.1 What You Can Do in this Chapter 187
9.1.2 What You Need to Know 188
9.2 Policy Route Screen 189
9.2.1 Policy Route Edit Screen 191
9.3 IP Static Route Screen 195
9.3.1 Static Route Add/Edit Screen 196
9.4 Policy Routing Technical Reference 197

Chapter 10
Routing Protocols 199

10.1 Routing Protocols Overview 199
10.1.1 What You Can Do in this Chapter 199
10.1.2 What You Need to Know 199
10.2 The RIP Screen 199
10.3 The OSPF Screen 201
10.3.1 Configuring the OSPF Screen 204
10.3.2 OSPF Area Add/Edit Screen 206
10.3.3 Virtual Link Add/Edit Screen 208
10.4 Routing Protocol Technical Reference 208

Chapter 11
Zones 211

11.1 Zones Overview 211
11.1.1 What You Can Do in this Chapter 211
11.1.2 What You Need to Know 211
11.2 The Zone Screen 212
11.3 Zone Edit 213

Chapter 12
DDNS 215

12.1 DDNS Overview 215
12.1.1 What You Can Do in this Chapter 215
12.1.2 What You Need to Know 215
12.2 The DDNS Screen 216
12.2.1 The Dynamic DNS Add/Edit Screen 217

Chapter 13
NAT 221

13.1 NAT Overview 221
13.1.1 What You Can Do in this Chapter 221
13.1.2 What You Need to Know 221
13.2 The NAT Screen 222
13.2.1 The NAT Add/Edit Screen 223
13.3 NAT Technical Reference 225

Chapter 14
HTTP Redirect 229

14.1 Overview 229
14.1.1 What You Can Do in this Chapter 229
14.1.2 What You Need to Know 229
14.2 The HTTP Redirect Screen 230
14.2.1 The HTTP Redirect Edit Screen 231

Chapter 15
ALG 233

15.1 ALG Overview 233
15.1.1 What You Can Do in this Chapter 233
15.1.2 What You Need to Know 233
15.1.3 Before You Begin 236
15.2 The ALG Screen 236
15.3 ALG Technical Reference 238

Chapter 16
IP/MAC Binding 241

16.1 IP/MAC Binding Overview 241
16.1.1 What You Can Do in this Chapter 241
16.1.2 What You Need to Know 241
16.2 IP/MAC Binding Summary 242
16.2.1 IP/MAC Binding Edit 242
16.2.2 Static DHCP Edit 243
16.3 IP/MAC Binding Exempt List 244

Chapter 17
Inbound Load Balancing 247

17.1 Inbound Load Balancing Overview 247
17.1.1 What You Can Do in this Chapter 247
17.2 The Inbound LB Screen 248
17.2.1 The Inbound LB Add/Edit Screen 249
17.2.2 The Inbound LB Member Add/Edit Screen 251

Chapter 18
Authentication Policy 253

18.1 Overview 253
18.1.1 What You Can Do in this Chapter 253
18.1.2 What You Need to Know 253
18.2 Authentication Policy Screen 254
18.2.1 Creating/Editing an Authentication Policy 256
18.3 User-aware Access Control Example 258
18.3.1 Set Up User Accounts 258
18.3.2 Set Up User Groups 259
18.3.3 Set Up User Authentication Using the RADIUS Server 259
18.3.4 User Group Authentication Using the RADIUS Server 261

Chapter 19
Firewall 265

19.1 Overview 265
19.1.1 What You Can Do in this Chapter 265
19.1.2 What You Need to Know 265
19.2 The Firewall Screen 268
19.2.1 Configuring the Firewall Screen 268
19.2.2 The Firewall Add/Edit Screen 272
19.3 The Session Limit Screen 273
19.3.1 The Session Limit Add/Edit Screen 275
19.4 Firewall Rule Configuration Example 276
19.5 Firewall Rule Example Applications 278

Chapter 20
IPSec VPN 281

20.1 Virtual Private Networks (VPN) Overview 281
20.1.1 What You Can Do in this Chapter 282
20.1.2 What You Need to Know 283
20.1.3 Before You Begin 284
20.2 The VPN Connection Screen 285
20.2.1 The VPN Connection Add/Edit (IKE) Screen 286
20.2.2 The VPN Connection Add/Edit Manual Key Screen 292
20.3 The VPN Gateway Screen 294
20.3.1 The VPN Gateway Add/Edit Screen 295
20.4 VPN Concentrator 301
20.4.1 VPN Concentrator Requirements and Suggestions 302
20.4.2 VPN Concentrator Screen 302
20.4.3 The VPN Concentrator Add/Edit Screen 302
20.5 ZyWALL IPSec VPN Client Configuration Provisioning 303
20.6 IPSec VPN Background Information 305

Chapter 21
SSL VPN 317

21.1 Overview 317
21.1.1 What You Can Do in this Chapter 317
21.1.2 What You Need to Know 317
21.2 The SSL Access Privilege Screen 318
21.2.1 The SSL Access Policy Add/Edit Screen 319
21.3 The SSL Global Setting Screen 322
21.3.1 How to Upload a Custom Logo 323
21.4 SSL VPN Example 324

Chapter 22
SSL User Screens 327

22.1 Overview 327
22.1.1 What You Need to Know 327
22.2 Remote SSL User Login 328
22.3 The SSL VPN User Screens 331
22.4 Bookmarking the ZyWALL 332
22.5 Logging Out of the SSL VPN User Screens 333
22.6 SSL User Application Screen 333
22.7 SSL User File Sharing 334
22.7.1 The Main File Sharing Screen 334
22.7.2 Opening a File or Folder 335
22.7.3 Downloading a File 336
22.7.4 Saving a File 336
22.7.5 Creating a New Folder 337
22.7.6 Renaming a File or Folder 337
22.7.7 Deleting a File or Folder 338
22.7.8 Uploading a File 338

Chapter 23
ZyWALL SecuExtender 341

23.1 The ZyWALL SecuExtender Icon 341
23.2 Status 341
23.3 View Log 342
23.4 Suspend and Resume the Connection 343
23.5 Stop the Connection 343
23.6 Uninstalling the ZyWALL SecuExtender 343

Chapter 24
L2TP VPN 345

24.1 Overview 345
24.1.1 What You Can Do in this Chapter 345

24.1.2 What You Need to Know 345
24.2 L2TP VPN Screen 347

Chapter 25
Bandwidth Management 349

25.1 Overview 349
25.1.1 What You Can Do in this Chapter 349
25.1.2 What You Need to Know 349
25.2 The Bandwidth Management Screen 353
25.2.1 The Bandwidth Management Add/Edit Screen 355

Chapter 26
Device HA 359

26.1 Overview 359
26.1.1 What You Can Do in this Chapter 359
26.1.2 What You Need to Know 359
26.1.3 Before You Begin 360
26.2 Device HA General 360
26.3 The Active-Passive Mode Screen 361
26.3.1 Configuring Active-Passive Mode Device HA 363
26.4 Configuring an Active-Passive Mode Monitored Interface 365
26.5 Device HA Technical Reference 366

Chapter 27
User/Group 371

27.1 Overview 371
27.1.1 What You Can Do in this Chapter 371
27.1.2 What You Need To Know 371
27.2 User Summary Screen 373
27.2.1 User Add/Edit Screen 374
27.3 User Group Summary Screen 376
27.3.1 Group Add/Edit Screen 377
27.4 The User/Group Setting Screen 378
27.4.1 Default User Authentication Timeout Settings Edit Screens 380
27.4.2 User Aware Login Example 381
27.5 User /Group Technical Reference 382

Chapter 28
Addresses 384

28.1 Overview 384
28.1.1 What You Can Do in this Chapter 384
28.1.2 What You Need To Know 384
28.2 Address Summary Screen 384

28.2.1 IPv4 Address Add/Edit Screen 386
28.2.2 IPv6 Address Add/Edit Screen 387
28.3 Address Group Summary Screen 388
28.3.1 Address Group Add/Edit Screen 389

Chapter 29
Services 390

29.1 Overview 390
29.1.1 What You Can Do in this Chapter 390
29.1.2 What You Need to Know 390
29.2 The Service Summary Screen 391
29.2.1 The Service Add/Edit Screen 392
29.3 The Service Group Summary Screen 393
29.3.1 The Service Group Add/Edit Screen 394

Chapter 30
Schedules 396

30.1 Overview 396
30.1.1 What You Can Do in this Chapter 396
30.1.2 What You Need to Know 396
30.2 The Schedule Summary Screen 397
30.2.1 The One-Time Schedule Add/Edit Screen 398
30.2.2 The Recurring Schedule Add/Edit Screen 399

Chapter 31
AAA Server 400

31.1 Overview 400
31.1.1 Directory Service (AD/LDAP) 400
31.1.2 RADIUS Server 400
31.1.3 ASAS 401
31.1.4 What You Can Do in this Chapter 401
31.1.5 What You Need To Know 401
31.2 Active Directory or LDAP Server Summary 403
31.2.1 Adding an Active Directory or LDAP Server 403
31.3 RADIUS Server Summary 406
31.3.1 Adding a RADIUS Server 406

Chapter 32
Authentication Method 409

32.1 Overview 409
32.1.1 What You Can Do in this Chapter 409
32.1.2 Before You Begin 409
32.1.3 Example: Selecting a VPN Authentication Method 409

32.2 Authentication Method Objects 410
32.2.1 Creating an Authentication Method Object 410

Chapter 33
Certificates 413

33.1 Overview 413
33.1.1 What You Can Do in this Chapter 413
33.1.2 What You Need to Know 413
33.1.3 Verifying a Certificate 415
33.2 The My Certificates Screen 416
33.2.1 The My Certificates Add Screen 417
33.2.2 The My Certificates Edit Screen 419
33.2.3 The My Certificates Import Screen 422
33.3 The Trusted Certificates Screen 423
33.3.1 The Trusted Certificates Edit Screen 424
33.3.2 The Trusted Certificates Import Screen 427
33.4 Certificates Technical Reference 428

Chapter 34
ISP Accounts 429

34.1 Overview 429
34.1.1 What You Can Do in this Chapter 429
34.2 ISP Account Summary 429
34.2.1 ISP Account Edit 430

Chapter 35
SSL Application 432

35.1 Overview 432
35.1.1 What You Can Do in this Chapter 432
35.1.2 What You Need to Know 432
35.1.3 Example: Specifying a Web Site for Access 433
35.2 The SSL Application Screen 434
35.2.1 Creating/Editing an SSL Application Object 435

Chapter 36
DHCPv6 438

36.1 Overview 438
36.1.1 What You Can Do in this Chapter 438
36.2 The DHCPv6 Request Screen 438
36.2.1 DHCPv6 Request Add/Edit Screen 439
36.3 The DHCPv6 Lease Screen 439
36.3.1 DHCPv6 Lease Add/Edit Screen 440

Chapter 37
System 443

37.1 Overview 443
37.1.1 What You Can Do in this Chapter 443
37.2 Host Name 444
37.3 USB Storage 444
37.4 Date and Time 445
37.4.1 Pre-defined NTP Time Servers List 448
37.4.2 Time Server Synchronization 448
37.5 Console Port Speed 449
37.6 DNS Overview 450
37.6.1 DNS Server Address Assignment 450
37.6.2 Configuring the DNS Screen 450
37.6.3 Address Record 452
37.6.4 PTR Record 452
37.6.5 Adding an Address/PTR Record 453
37.6.6 Domain Zone Forwarder 453
37.6.7 Adding a Domain Zone Forwarder 453
37.6.8 MX Record 454
37.6.9 Adding a MX Record 454
37.6.10 Adding a DNS Service Control Rule 455
37.7 WWW Overview 456
37.7.1 Service Access Limitations 456
37.7.2 System Timeout 456
37.7.3 HTTPS 456
37.7.4 Configuring WWW Service Control 457
37.7.5 Service Control Rules 460
37.7.6 Customizing the WWW Login Page 461
37.7.7 HTTPS Example 465
37.8 SSH 472
37.8.1 How SSH Works 473
37.8.2 SSH Implementation on the ZyWALL 474
37.8.3 Requirements for Using SSH 474
37.8.4 Configuring SSH 474
37.8.5 Secure Telnet Using SSH Examples 475
37.9 Telnet 476
37.9.1 Configuring Telnet 476
37.10 FTP 478
37.10.1 Configuring FTP 478
37.11 SNMP 479
37.11.1 Supported MIBs 480
37.11.2 SNMP Traps 481
37.11.3 Configuring SNMP 481

37.12 Language Screen 483
37.13 IPv6 Screen 483

Chapter 38
Log and Report 485

38.1 Overview 485
38.1.1 What You Can Do In this Chapter 485
38.2 Email Daily Report 485
38.3 Log Setting Screens 487
38.3.1 Log Setting Summary 487
38.3.2 Edit System Log Settings 489
38.3.3 Edit Log on USB Storage Setting 491
38.3.4 Edit Remote Server Log Settings 493
38.3.5 Log Category Settings Screen 495

Chapter 39
File Manager 499

39.1 Overview 499
39.1.1 What You Can Do in this Chapter 499
39.1.2 What you Need to Know 499
39.2 The Configuration File Screen 501
39.3 The Firmware Package Screen 505
39.4 The Shell Script Screen 507

Chapter 40
Diagnostics 510

40.1 Overview 510
40.1.1 What You Can Do in this Chapter 510
40.2 The Diagnostic Screen 510
40.2.1 The Diagnostics Files Screen 511
40.3 The Packet Capture Screen 512
40.3.1 The Packet Capture Files Screen 514
40.4 Core Dump Screen 515
40.4.1 Core Dump Files Screen 516
40.5 The System Log Screen 516

Chapter 41
Packet Flow Explore 518

41.1 Overview 518
41.1.1 What You Can Do in this Chapter 518
41.2 The Routing Status Screen 518
41.3 The SNAT Status Screen 522

Chapter 42
Reboot 525

42.1 Overview 525
42.1.1 What You Need To Know 525
42.2 The Reboot Screen 525

Chapter 43
Shutdown 526

43.1 Overview 526
43.1.1 What You Need To Know 526
43.2 The Shutdown Screen 526

Chapter 44
Troubleshooting 527

44.1 Resetting the ZyWALL 535
44.2 Getting More Troubleshooting Help 536

Appendix A Legal Information 537

Index 541

1

Introduction

1.1 Overview

Note: This help covers the following ZyWALL models and refers to them all as “ZyWALL”.

Features and interface names vary by model. Key feature differences between ZyWALL models are as follows. Other features are common to all models although features may vary slightly by model. See the specific product’s datasheet for detailed specifications.

Table 1 Model-Specific Features

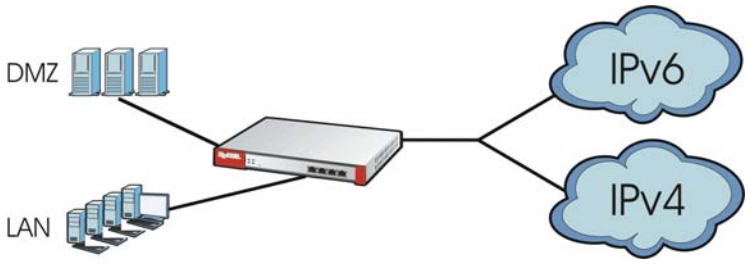
FEATURE	ZYWALL
Rack-mounting	110, 310, 1100
Wall-mounting	110
Port Role	110
Compact Flash Card Slot	110

Here are some ZyWALL application scenarios.

IPv6 Routing

The ZyWALL supports IPv6 Ethernet, PPP, VLAN, and bridge routing. You may also create IPv6 policy routes and IPv6 objects. The ZyWALL can also route IPv6 packets through IPv4 networks using different tunneling methods.

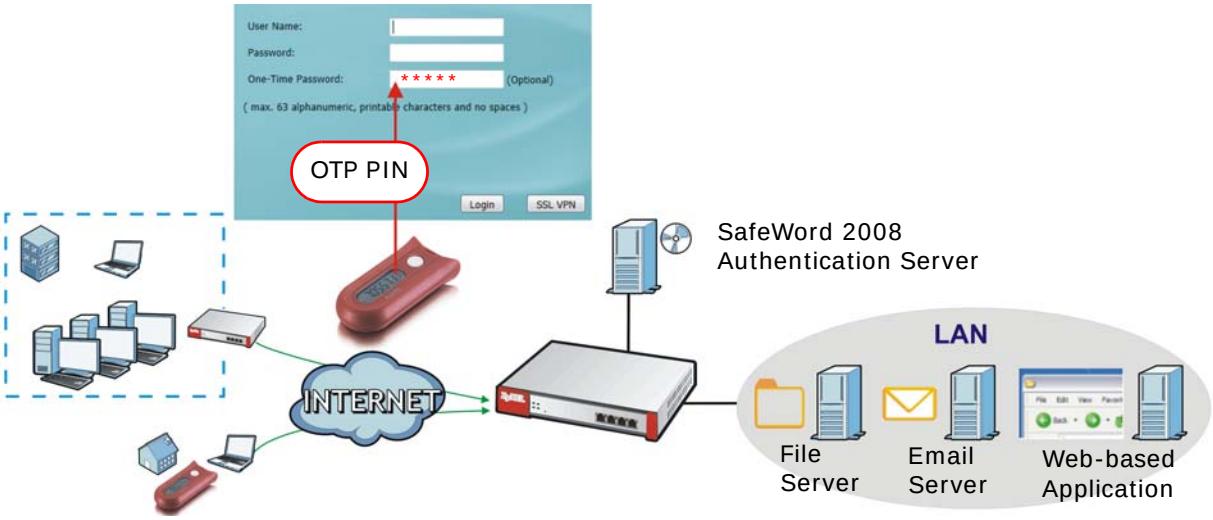
Figure 1 Applications: IPv6 Routing



VPN Connectivity

Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also purchase the ZyWALL OTPv2 One-Time Password System for strong two-factor authentication for Web Configurator, Web access, SSL VPN, and ZyXEL IPSec VPN client user logins.

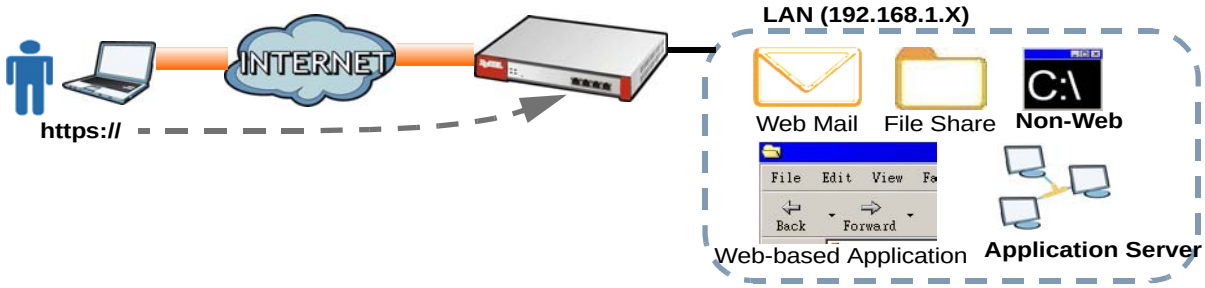
Figure 2 Applications: VPN Connectivity



SSL VPN Network Access

SSL VPN lets remote users use their web browsers for a very easy-to-use VPN solution. A user just browses to the ZyWALL's web address and enters his user name and password to securely connect to the ZyWALL's network. Here full tunnel mode creates a virtual connection for a remote user and gives him a private IP address in the same subnet as the local network so he can access network resources in the same way as if he were part of the internal network.

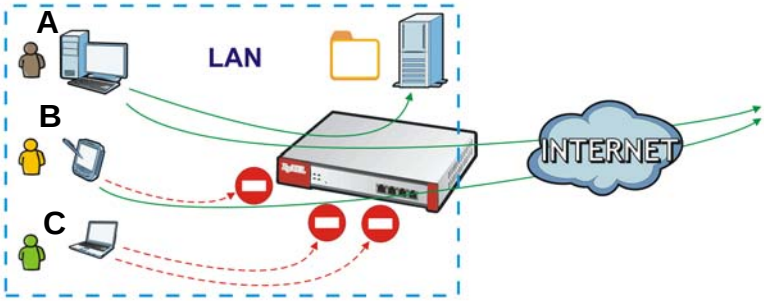
Figure 3 SSL VPN With Full Tunnel Mode



User-Aware Access Control

Set up security policies to restrict access to sensitive information and shared resources based on the user who is trying to access it. In the following figure user **A** can access both the Internet and an internal file server. User **B** has a lower level of access and can only access the Internet. User **C** is not even logged in and cannot access either.

Figure 4 Applications: User-Aware Access Control



Load Balancing

Set up multiple connections to the Internet on the same port, or different ports, including cellular interfaces. In either case, you can balance the traffic loads between them.

Figure 5 Applications: Multiple WAN Interfaces



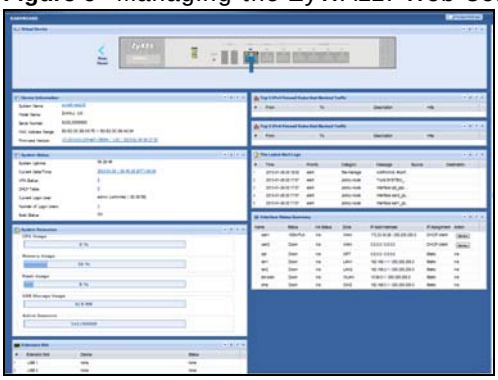
1.2 Management Overview

You can manage the ZyWALL in the following ways.

Web Configurator

The Web Configurator allows easy ZyWALL setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

Figure 6 Managing the ZyWALL: Web Configurator



Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the ZyWALL. Access it using remote management (for example, SSH or Telnet) or via the physical or Web Configurator console port. See the Command Reference Guide for CLI details. The default settings for the console port are:

Table 2 Console Port Default Settings

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

1.3 Web Configurator

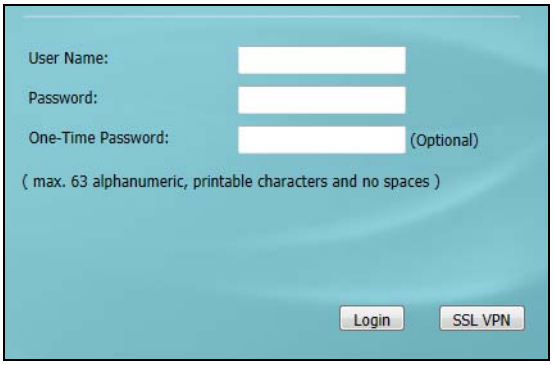
In order to use the Web Configurator, you must:

- Use one of the following web browser versions or later: Internet Explorer 7, Firefox 3.5, Chrome 9.0
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts, Java permissions, and cookies

The recommended screen resolution is 1024 x 768 pixels.

1.3.1 Web Configurator Access

1. Make sure your ZyWALL hardware is properly connected. See the Quick Start Guide.
2. In your browser go to http://192.168.1.1. By default, the ZyWALL automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.

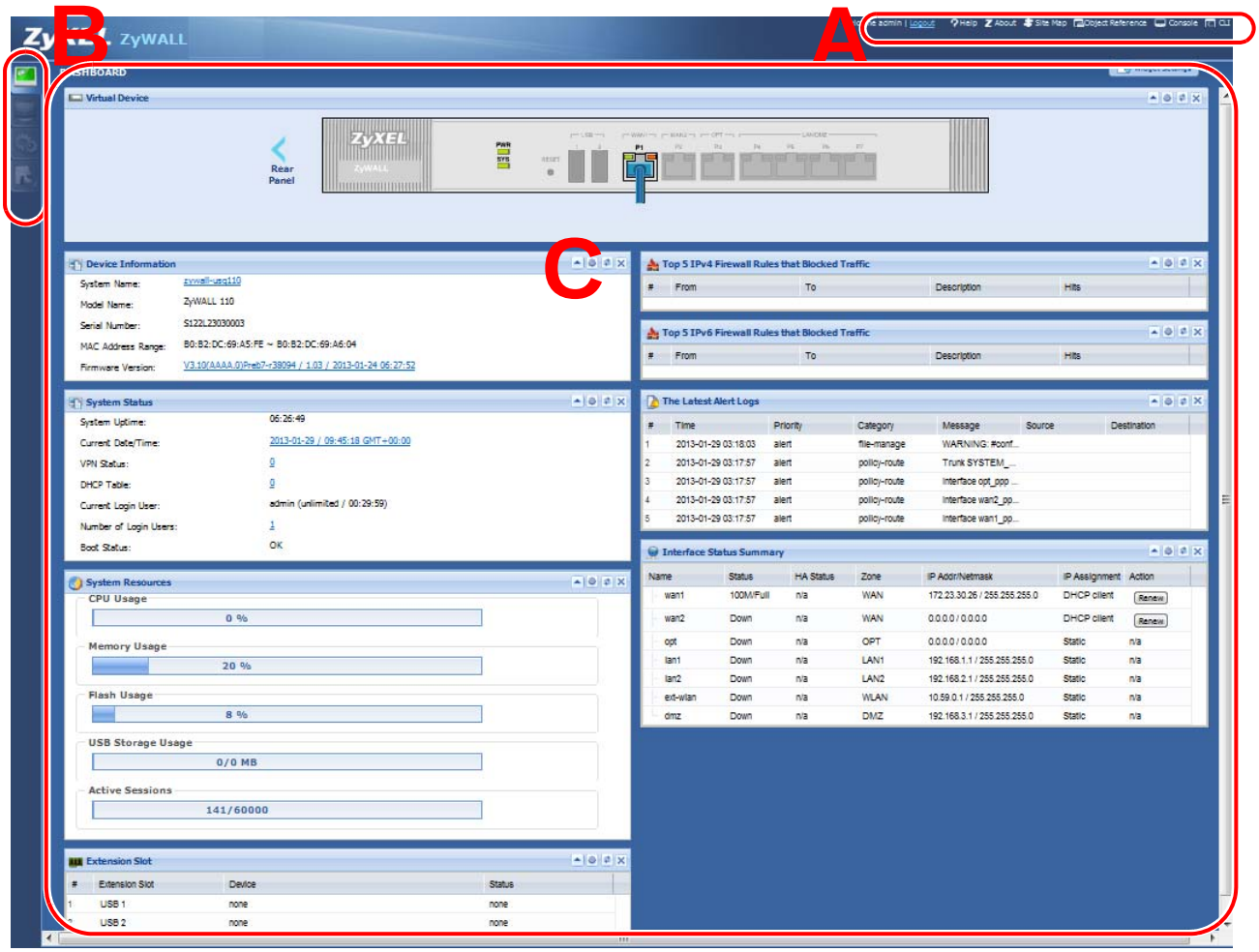


3. Type the user name (default: “admin”) and password (default: “1234”).

   If you have a OTP (One-Time Password) token generate a number and enter it in the **One-Time Password** field. The number is only good for one login. You must use the token to generate a new number the next time you log in.

4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.

5 Follow the directions in the **Update Admin Info** screen. If you change the default password, the **Login** screen appears after you click **Apply**. If you click **Ignore**, the **Installation Setup Wizard** opens if the ZyWALL is using its default configuration; otherwise the dashboard appears.



1.3.2 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts (as illustrated on page 21):

- **A** - title bar
- **B** - navigation panel
- **C** - main window

Title Bar

Figure 7 Title Bar



The title bar icons in the upper right corner provide the following functions.

Table 3 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Help	Click this to open the help page for the current screen.
About	Click this to display basic information about the ZyWALL.
Site Map	Click this to see an overview of links to the Web Configurator screens.
Object Reference	Click this to check which configuration items reference an object.
Console	Click this to open a Java-based console window from which you can run command line interface (CLI) commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator to the ZyWALL.

About

Click **About** to display basic information about the ZyWALL.

Figure 8 About

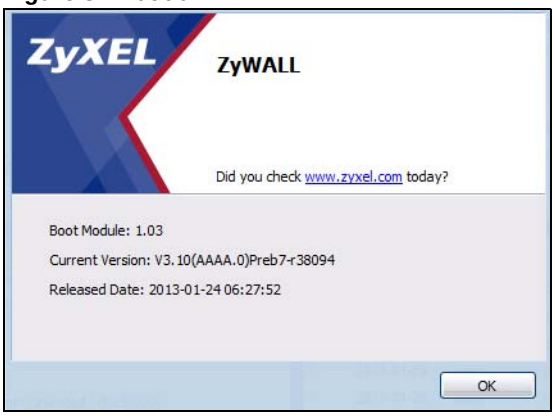


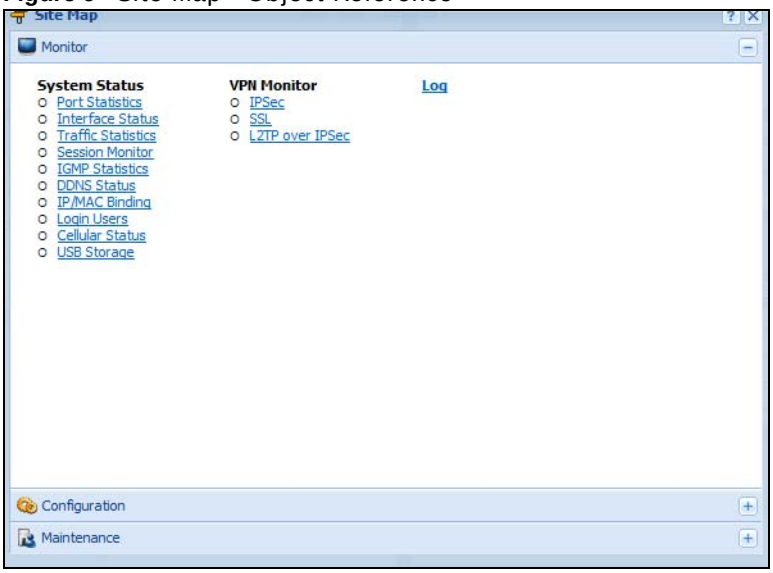
Table 4 About

LABEL	DESCRIPTION
Boot Module	This shows the version number of the software that handles the booting process of the ZyWALL.
Current Version	This shows the firmware version of the ZyWALL.
Released Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
OK	Click this to close the screen.

Site Map

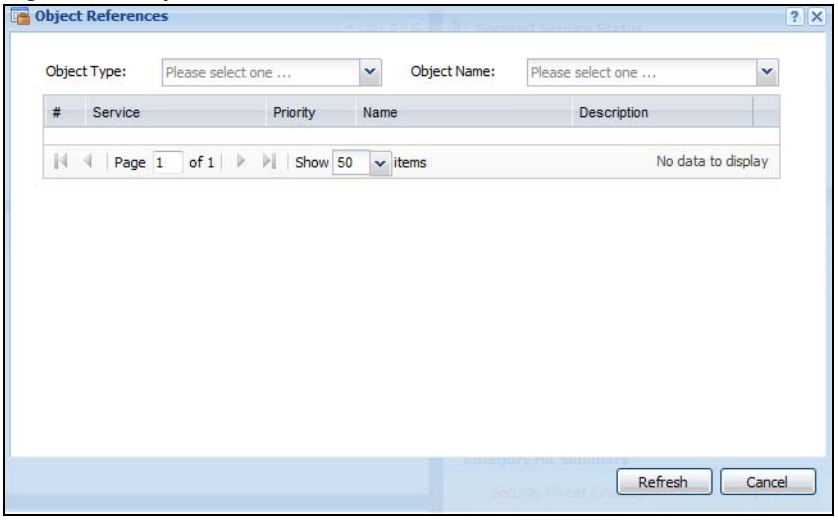
Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

Figure 9 Site Map Object Reference



Click **Object Reference** to open the **Object Reference** screen. Select the type of object and the individual object and click **Refresh** to show which configuration settings reference the object.

Figure 10 Object Reference



The fields vary with the type of object. This table describes labels that can appear in this screen.

Table 5 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.

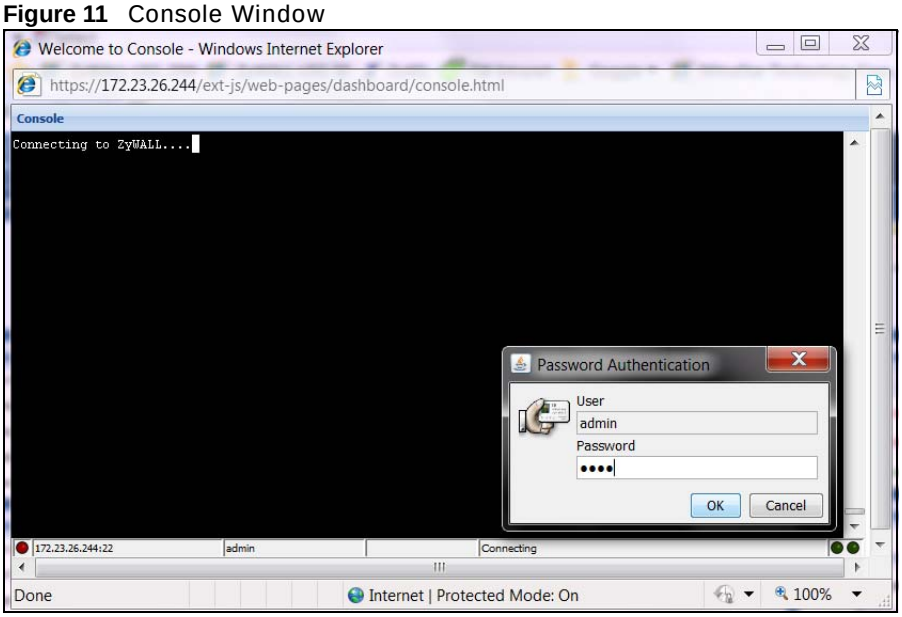
Table 5 Object References (continued)

LABEL	DESCRIPTION
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

Console

Click **Console** to open a Java-based console window from which you can run CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands.

Figure 11 Console Window



CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. Open the pop-up window and then click some menus in the web configurator to dislay the corresponding commands.

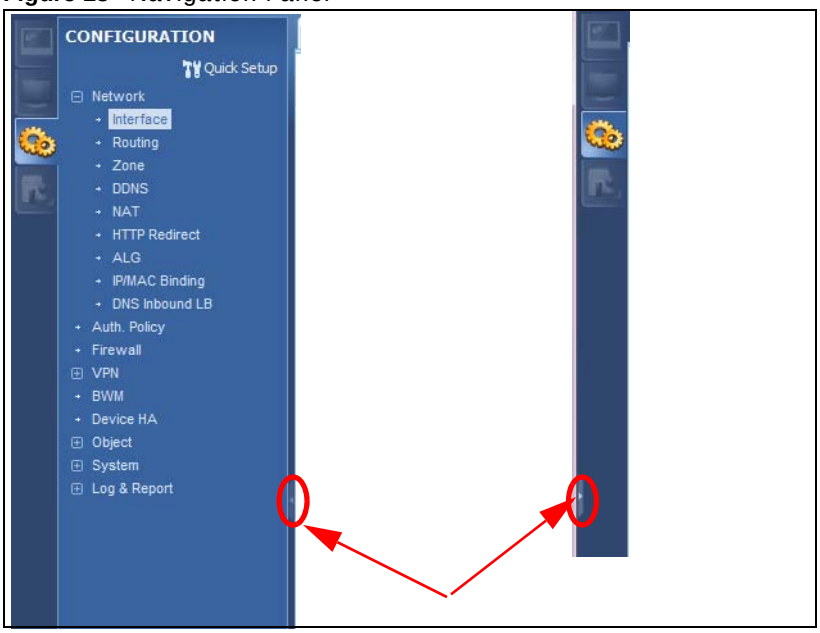
Figure 12 CLI Messages



1.3.3 Navigation Panel

Use the navigation panel menu items to open status and configuration screens. Click the arrow in the middle of the right edge of the navigation panel to hide the panel or drag to resize it. The following sections introduce the ZyWALL's navigation panel menus and their screens.

Figure 13 Navigation Panel



Dashboard

The dashboard displays general device information, system status, system resource usage,, and interface status in widgets that you can re-arrange to suit your needs. See the Web Help for details on the dashboard.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 6 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System Status		
Port Statistics		Displays packet statistics for each physical port.
Interface Status		Displays general interface information and packet statistics.
Traffic Statistics		Collect and display traffic statistics.
Session Monitor		Displays the status of all current sessions.
DDNS Status		Displays the status of the ZyWALL's DDNS domain names.
IP/MAC Binding		Lists the devices that have received an IP address from ZyWALL interfaces using IP/MAC binding.
Login Users		Lists the users currently logged into the ZyWALL.

Table 6 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Cellular Status		Displays details about the ZyWALL's 3G connection status.
USB Storage		Displays details about USB device connected to the ZyWALL.
VPN Monitor		
IPSec		Displays and manages the active IPSec SAs.
SSL		Lists users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
L2TP over IPSec		Displays details about current L2TP sessions.
Log		Lists log entries.

Configuration Menu

Use the configuration menu screens to configure the ZyWALL's features.

Table 7 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Quick Setup		Quickly configure WAN interfaces or VPN connections.
Network		
Interface	Port Role	Use this screen to set the ZyWALL's flexible ports as LAN1, WLAN, or DMZ.
	Ethernet	Manage Ethernet interfaces and virtual Ethernet interfaces.
	PPP	Create and manage PPPoE and PPTP interfaces.
	Cellular	Configure a cellular Internet connection for an installed 3G card.
	Tunnel	Configure tunneling between IPv4 and IPv6 networks.
	VLAN	Create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Create and manage bridges and virtual bridge interfaces.
	Trunk	Create and manage trunks (groups of interfaces) for load balancing.
Routing	Policy Route	Create and manage routing policies.
	Static Route	Create and manage IP static routing information.
	RIP	Configure device-level RIP settings.
	OSPF	Configure device-level OSPF settings, including areas and virtual links.
Zone		Configure zones used to define various policies.
DDNS	DDNS	Define and manage the ZyWALL's DDNS domain names.
NAT		Set up and manage port forwarding rules.
HTTP Redirect		Set up and manage HTTP redirection rules.
ALG		Configure SIP, H.323, and FTP pass-through settings.
IP/MAC Binding	Summary	Configure IP to MAC address bindings for devices connected to each supported interface.
	Exempt List	Configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding.
DNS Inbound LB	DNS Load Balancing	Configure DNS Load Balancing.
Auth. Policy		Define rules to force user authentication.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Firewall	Firewall	Create and manage level-3 traffic rules.
	Session Control	Limit the number of concurrent client NAT/firewall sessions.
VPN		
IPSec VPN	VPN Connection	Configure IPSec tunnels.
	VPN Gateway	Configure IKE tunnels.
	Concentrator	Combine IPSec VPN connections into a single secure network
	Configuration Provisioning	Set who can retrieve VPN rule settings from the ZyWALL using the ZyWALL IPSec VPN Client.
SSL VPN	Access Privilege	Configure SSL VPN access rights for users and groups.
	Global Setting	Configure the ZyWALL's SSL VPN settings that apply to all connections.
L2TP VPN	L2TP VPN	Configure L2TP over IPSec tunnels.
BWM	BWM	Enable and configure bandwidth management rules.
Device HA	General	Configure device HA global settings, and see the status of each interface monitored by device HA.
	Active-Passive Mode	Configure active-passive mode device HA.
Object		
User/Group	User	Create and manage users.
	Group	Create and manage groups of users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
Address	Address	Create and manage host, range, and network (subnet) addresses.
	Address Group	Create and manage groups of addresses.
Service	Service	Create and manage TCP and UDP services.
	Service Group	Create and manage groups of services.
Schedule	Schedule	Create one-time and recurring schedules.
AAA Server	Active Directory	Configure the Active Directory settings.
	LDAP	Configure the LDAP settings.
	RADIUS	Configure the RADIUS settings.
Auth. Method	Authentication Method	Create and manage ways of authenticating users.
Certificate	My Certificates	Create and manage the ZyWALL's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
ISP Account	ISP Account	Create and manage ISP account information for PPPoE/PPTP interfaces.
SSL Application		Create SSL web application objects.
DHCPv6	Request	Configure IPv6 DHCP request type and interface information.
	Lease	Configure IPv6 DHCP lease type and interface information.
System		
Host Name		Configure the system and domain name for the ZyWALL.
USB Storage	Settings	Configure the settings for the connected USB devices.
Date/Time		Configure the current date, time, and time zone in the ZyWALL.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Console Speed		Set the console speed.
DNS		Configure the DNS server and address records for the ZyWALL.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
	Login Page	Configure how the login and access user screens look.
SSH		Configure SSH server and SSH service settings.
TELNET		Configure telnet server settings for the ZyWALL.
FTP		Configure FTP server settings.
SNMP		Configure SNMP communities and services.
Language		Select the Web Configurator language.
IPv6		Enable IPv6 globally on the ZyWALL here.
Log & Report		
Email Daily Report		Configure where and how to send daily reports and what reports to send.
Log Settings		Configure the system log, e-mail logs, and remote syslog servers.

Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the ZyWALL.

Table 8 Maintenance Menu Screens Summary

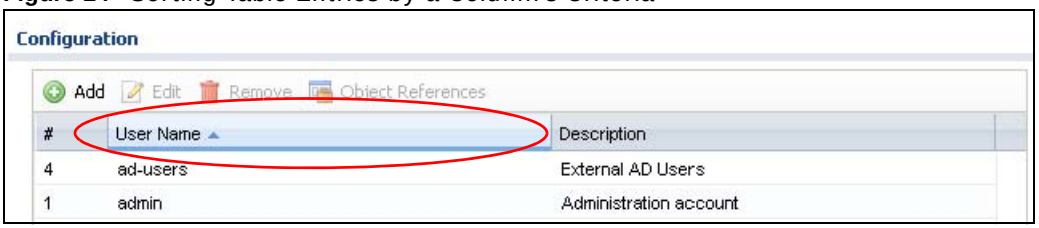
FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the ZyWALL.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the ZyWALL.
Diagnostics	Diagnostic	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	Core Dump	Connect a USB device to the ZyWALL and save the ZyWALL operating system kernel to it here.
	System Log	Connect a USB device to the ZyWALL and archive the ZyWALL system logs to it here.
Packet Flow Explore	Routing Status	Check how the ZyWALL determines where to route a packet.
	SNAT Status	View a clear picture on how the ZyWALL converts a packet's source IP address and check the related settings.
Reboot		Restart the ZyWALL.
Shutdown		Turn off the ZyWALL.

1.3.4 Tables and Lists

Web Configurator tables and lists are flexible with several options for how to display their entries.

Click a column heading to sort the table's entries according to that column's criteria.

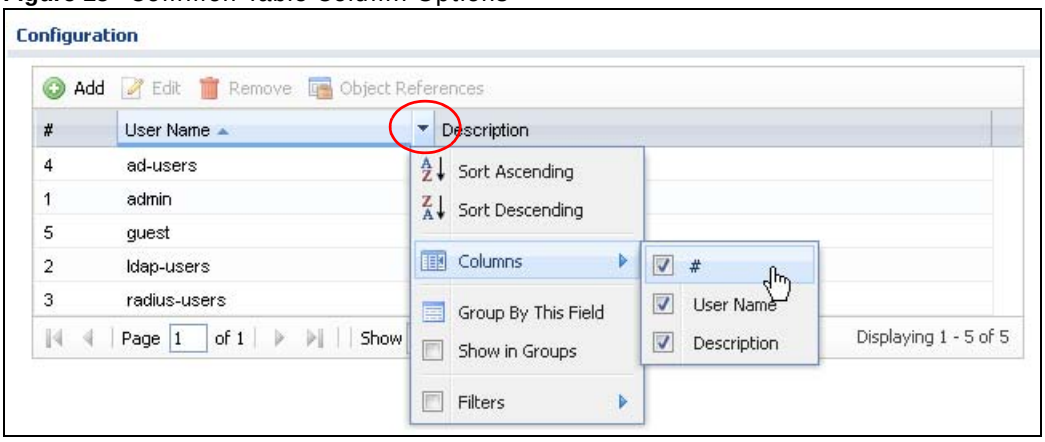
Figure 14 Sorting Table Entries by a Column's Criteria



Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

Figure 15 Common Table Column Options



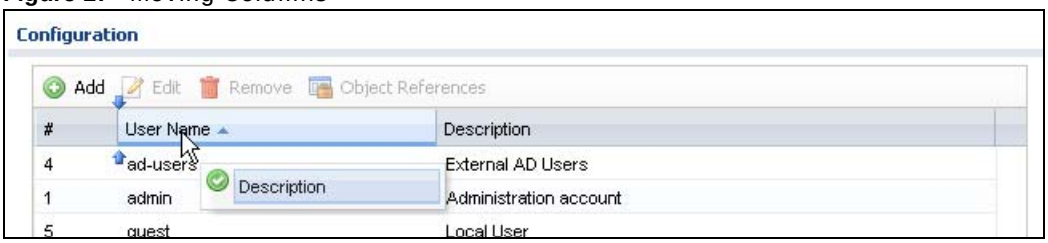
Select a column heading cell's right border and drag to re-size the column.

Figure 16 Resizing a Table Column



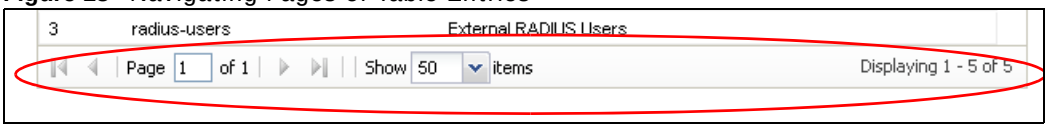
Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

Figure 17 Moving Columns



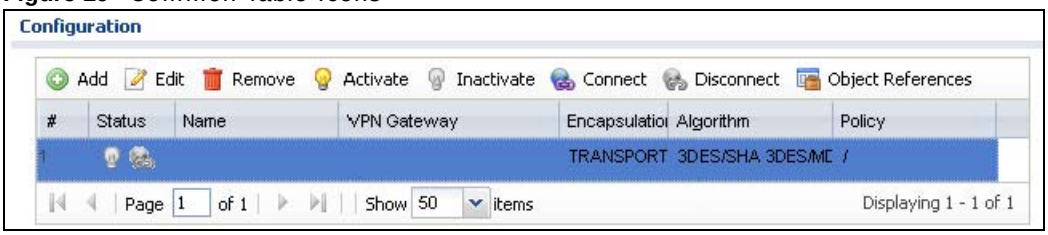
Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

Figure 18 Navigating Pages of Table Entries



The tables have icons for working with table entries. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

Figure 19 Common Table Icons



Here are descriptions for the most common table icons.

Table 9 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the ZyWALL applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an entry, select it and click **Connect**.
Disconnect	To disconnect an entry, select it and click **Disconnect**.
Object References	Select an entry and click **Object References** to check which settings use the entry.
Move	To change an entry's position in a numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.

Working with Lists

When a list of available entries displays next to a list of selected entries, you can often just double-click an entry to move it from one list to the other. In some lists you can also use the [Shift] or [Ctrl] key to select multiple entries, and then use the arrow button to move them to the other list.

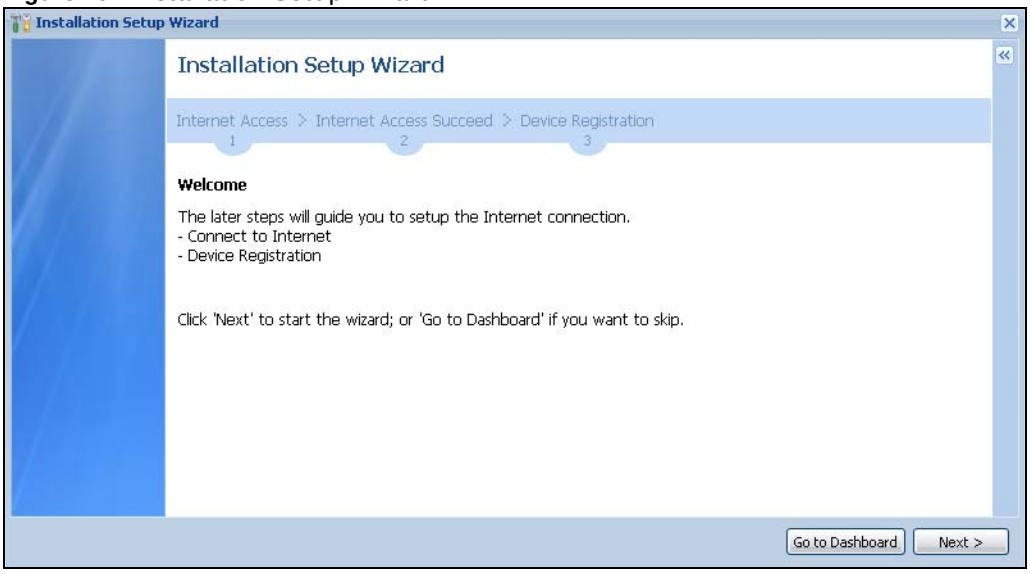
2

Installation Setup Wizard

2.1 Installation Setup Wizard Screens

When you log into the Web Configurator for the first time or when you reset the ZyWALL to its default configuration, the **Installation Setup Wizard** screen displays. This wizard helps you configure Internet connection settings and activate subscription services. This chapter provides information on configuring the Web Configurator's installation setup wizard. See the feature-specific chapters in this User's Guide for background information.

Figure 20 Installation Setup Wizard


Installation Setup Wizard
Installation Setup Wizard
Internet Access > Internet Access Succeed > Device Registration
1
2
3
Welcome
The later steps will guide you to setup the Internet connection.
- Connect to Internet
- Device Registration
Click 'Next' to start the wizard; or 'Go to Dashboard' if you want to skip.
Go to Dashboard
Next >

- Click the double arrow in the upper right corner to display or hide the help.
- Click **Go to Dashboard** to skip the installation setup wizard or click **Next** to start configuring for Internet access.

2.1.1 Internet Access Setup - WAN Interface

Use this screen to configure the WAN interface's type of encapsulation and method of IP address assignment.

The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

- **Encapsulation**: Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

- **WAN Interface**: This is the interface you are configuring for Internet access.
- **Zone**: This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment**: Select **Auto** if your ISP did not assign you a fixed IP address. Select **Static** if the ISP assigned a fixed IP address.

2.1.2 Internet Access: Ethernet

This screen is read-only if you set the previous screen's **IP Address Assignment** field to **Auto**. Use this screen to configure your IP address settings.

Note: Enter the Internet access information exactly as given to you by your ISP.

- **Encapsulation**: This displays the type of Internet connection you are configuring.
- **First WAN Interface**: This is the number of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.

The following fields display if you selected static IP address assignment.

- **IP Subnet Mask**: Enter the subnet mask for this WAN connection's IP address.
- **Gateway IP Address**: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.3 Internet Access: PPPoE

Note: Enter the Internet access information exactly as given to you by your ISP.

2.1.3.1 ISP Parameters

- Type the PPPoE **Service Name** from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long.
- **Authentication Type** - Select an authentication protocol for outgoing connection requests. Options are:
  - **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by the remote node.
  - **CHAP** - Your ZyWALL accepts CHAP only.
  - **PAP** - Your ZyWALL accepts PAP only.
  - **MSCHAP** - Your ZyWALL accepts MSCHAP only.
  - **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.

- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPPoE server.

2.1.3.2 WAN IP Address Assignments

- **WAN Interface**: This is the name of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

2.1.4 Internet Access: PPTP

Note: Enter the Internet access information exactly as given to you by your ISP.

2.1.5 ISP Parameters

- **Authentication Type** - Select an authentication protocol for outgoing calls. Options are:
  - **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by the remote node.
  - **CHAP** - Your ZyWALL accepts CHAP only.
  - **PAP** - Your ZyWALL accepts PAP only.
  - **MSCHAP** - Your ZyWALL accepts MSCHAP only.
  - **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank. Re-type your password in the next field to confirm it.
- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPTP server.

2.1.5.1 PPTP Configuration

- **Base Interface**: This identifies the Ethernet interface you configure to connect with a modem or router.
- Type a **Base IP Address** (static) assigned to you by your ISP.
- Type the **IP Subnet Mask** assigned to you by your ISP (if given).
- **Server IP**: Type the IP address of the PPTP server.

- Type a **Connection ID** or connection name. It must follow the “c:id” and “n:name” format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your broadband modem or router. You can use alphanumeric and -_: characters, and it can be up to 31 characters long.

2.1.5.2 WAN IP Address Assignments

- **First WAN Interface**: This is the connection type on the interface you are configuring to connect with your ISP.
- **Zone** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. Auto displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

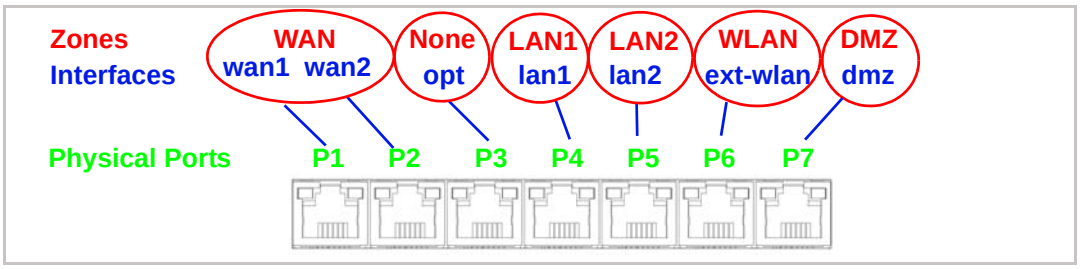
2.1.6 Internet Access - Finish

You have set up your ZyWALL to access the Internet. A screen displays with your settings. If they are not correct, click **Back**.

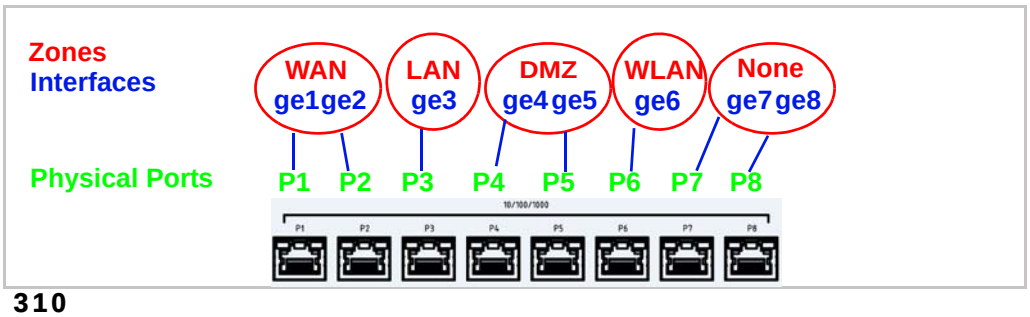
3.1 Default Zones, Interfaces, and Ports

The default configurations for zones, interfaces, and ports are as follows. References to interfaces may be generic rather than the specific name used in your model. For example, this guide may use "the WAN interface" rather than "wan1" or "wan2", "ge2" or" ge3".

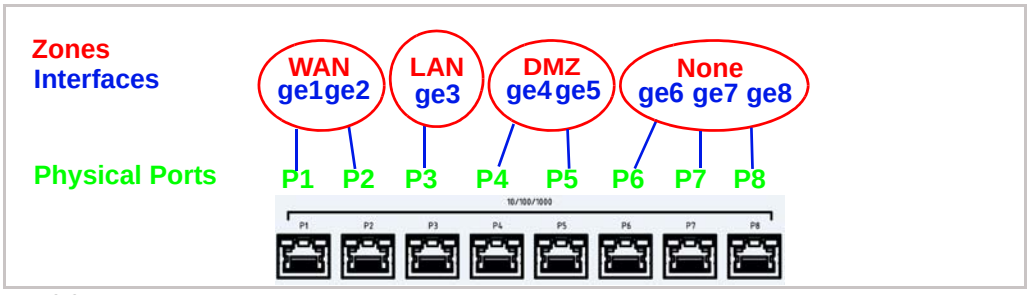
An OPT (optional) Ethernet port can be configured as an additional WAN port, LAN, WLAN, or DMZ port.



110



310



1100

Note: Use an 8-wire Ethernet cable to run your Gigabit Ethernet at 1000 Mbps. Using a 4-wire Ethernet cable limits your connection to 100 Mbps. Note that the connection speed also depends on what the Ethernet device at the other end can support.

3.2 Stopping the ZyWALL

Always use **Maintenance > Shutdown > Shutdown** or the shutdown command before you turn off the ZyWALL or remove the power. Not doing so can cause the firmware to become corrupt.

3.3 Rack-mounting

See Chapter 1 on page 17 for the ZyWALL models that can be rack mounted. Use the following steps to mount the ZyWALL on an EIA standard size, 19-inch rack or in a wiring closet with other equipment using a rack-mounting kit. Make sure the rack will safely support the combined weight of all the equipment it contains and that the position of the ZyWALL does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

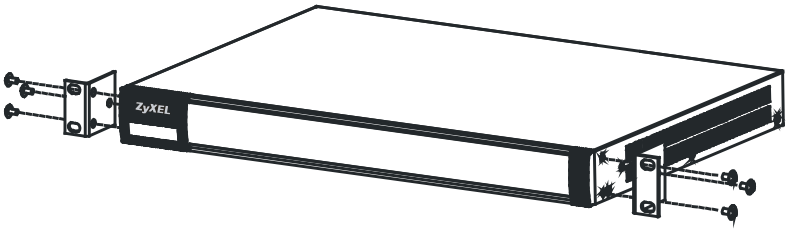
Note: Leave 10 cm of clearance at the sides and 20 cm in the rear.

Use a #2 Phillips screwdriver to install the screws.

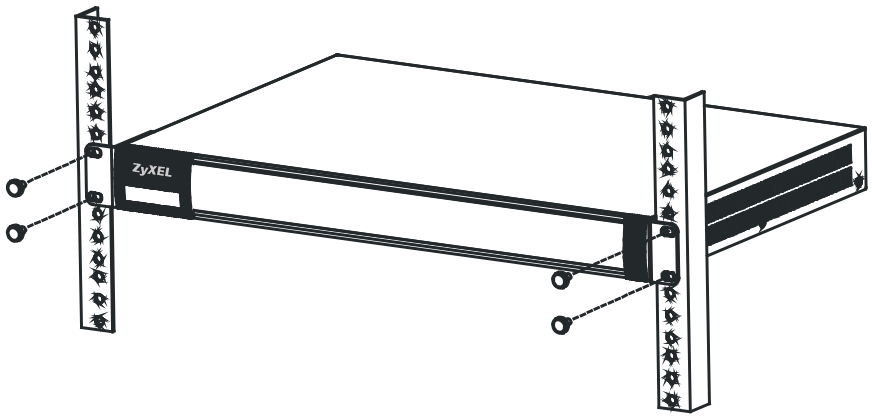
Note: Failure to use the proper screws may damage the unit.

1 Align one bracket with the holes on one side of the ZyWALL and secure it with the included bracket screws (smaller than the rack-mounting screws).

2 Attach the other bracket in a similar fashion.



3 After attaching both mounting brackets, position the ZyWALL in the rack and up the bracket holes with the rack holes. Secure the ZyWALL to the rack with the rack-mounting screws.



3.4 Wall-mounting

See Chapter 1 on page 17 for the ZyWALL models that can be wall-mounted. Do the following to attach your ZyWALL to a wall.

1 Screw two screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads into the wall 150 mm apart (see the figure in step 2). Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

The gap must be big enough for the screw heads to slide into the screw slots and the connection cables to run down the back of the ZyWALL.

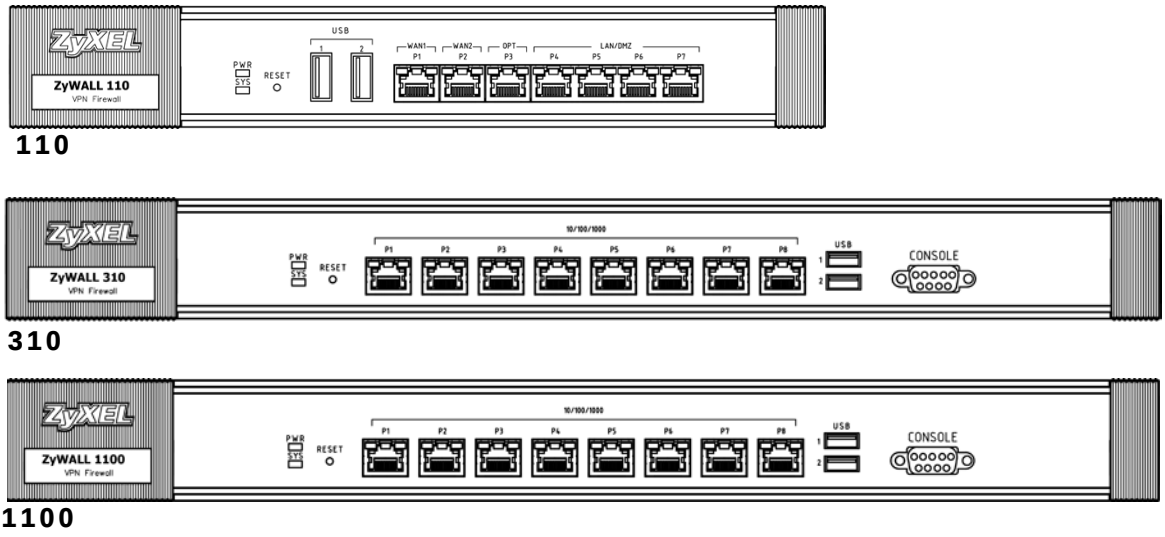
Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the ZyWALL with the connection cables.

2 Use the holes on the bottom of the ZyWALL to hang the ZyWALL on the screws.

3.5 Front Panel LEDs

This section introduces the ZyWALL's front panel LEDs.

Figure 21 ZyWALL Front Panel



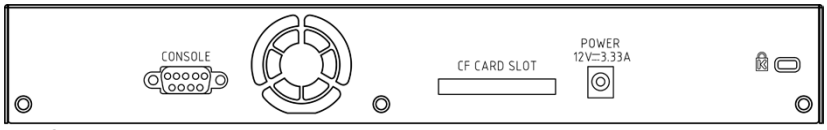
The following tables describe the LEDs.

Table 10 Front Panel LEDs

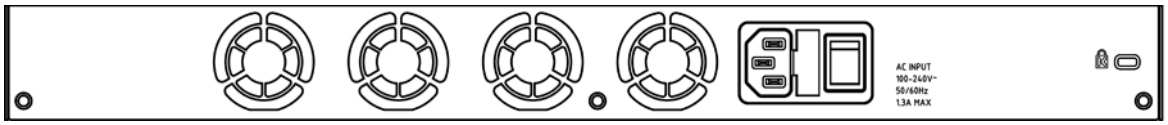
LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 3.2 on page 38). If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The ZyWALL is not ready or has failed.
		On	The ZyWALL is ready and running.
		Blinking	The ZyWALL is booting.
	Red	On	The ZyWALL xd an error or has failed.
USB	Green	Off	No device is connected to the ZyWALL's USB port or the connected device is not supported by the ZyWALL.
		On	A 3G USB card or USB storage device is connected to the USB port.
	Orange	On	Connected to a 3G network through the connected 3G USB card.
P1, P2...	Green	Off	There is no traffic on this port.
		Blinking	The ZyWALL is sending or receiving packets on this port.
	Orange	Off	There is no connection on this port.
		On	This port has a successful link.

3.5.1 Rear Panels

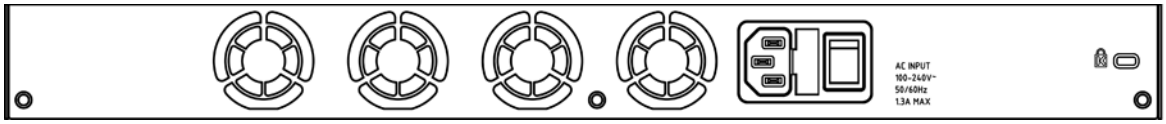
The following graphic shows the rear panel of the ZyWALL.



110



310



1100

Table 11 Rear Panel

LABEL	DESCRIPTION
Console	You can use the console port to manage the ZyWALL using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
CF Card Slot	Insert a compact flash card into this slot to store ZyWALL system logs.
Power	Use the included power cord to connect the power socket to a power outlet. Turn the power switch on if your ZyWALL has a power switch.
Lock	Attach a lock-and-cable from the Kensington lock (the small, metal-reinforced, oval hole) to a permanent object, such as a pole, to secure the ZyWALL in place.
Fan	The fans are for cooling the ZyWALL. Make sure they are not obstructed to allow maximum ventilation.

4

Quick Setup Wizards

4.1 Quick Setup Overview

The Web Configurator's quick setup wizards help you configure Internet and VPN connection settings. This chapter provides information on configuring the quick setup screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

In the Web Configurator, click **Configuration > Quick Setup** to open the first **Quick Setup** screen.

Figure 22 Quick Setup


Quick Setup
WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.
VPN Setup
For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

- **WAN Interface**

  Click this link to open a wizard to set up a WAN (Internet) connection. This wizard creates matching ISP account settings in the ZyWALL if you use PPPoE or PPTP. See Section 4.2 on page 43.

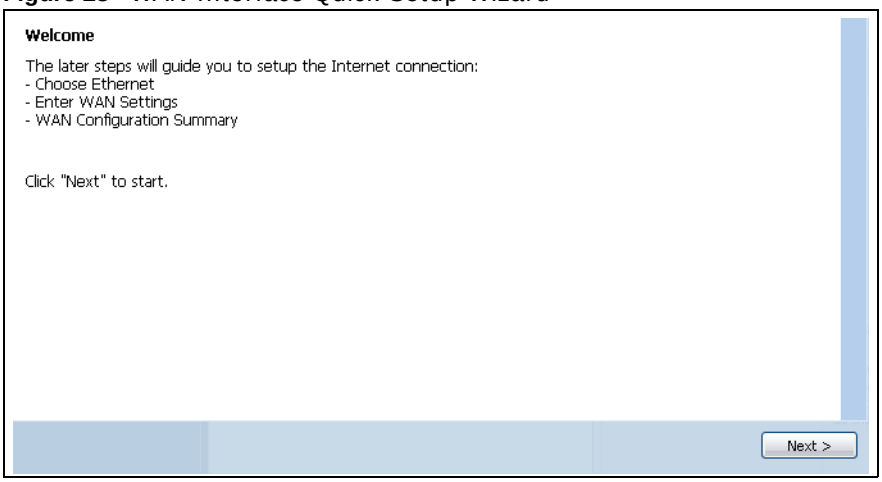
- **VPN SETUP**

  Use **VPN Setup** to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. **Use VPN Settings for Configuration Provisioning** to set up a VPN rule that can be retrieved with the ZyWALL IPSec VPN Client. You only need to enter a user name, password and the IP address of the ZyWALL in the ZyWALL IPSec VPN Client to get all VPN settings automatically from the ZyWALL. See Section 4.3 on page 48.

4.2 WAN Interface Quick Setup

Click **WAN Interface** in the main **Quick Setup** screen to open the **WAN Interface Quick Setup Wizard Welcome** screen. Use these screens to configure an interface to connect to the Internet. Click **Next**.

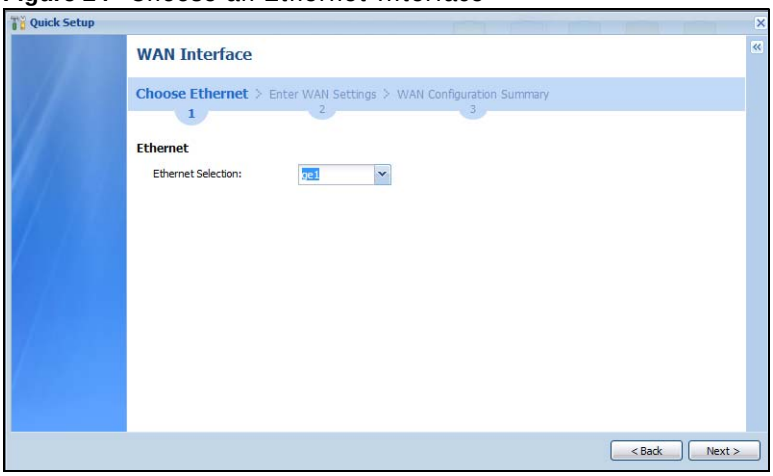
Figure 23 WAN Interface Quick Setup Wizard


Welcome
The later steps will guide you to setup the Internet connection:
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary
Click "Next" to start.
Next >

4.2.1 Choose an Ethernet Interface

Select the Ethernet interface that you want to configure for a WAN connection and click **Next**.

Figure 24 Choose an Ethernet Interface

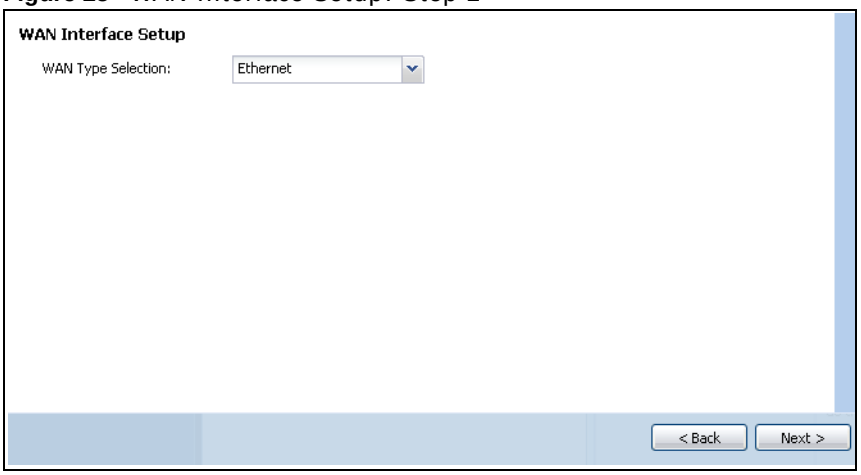


4.2.2 Select WAN Type

WAN Type Selection: Select the type of encapsulation this connection is to use. Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

Figure 25 WAN Interface Setup: Step 2



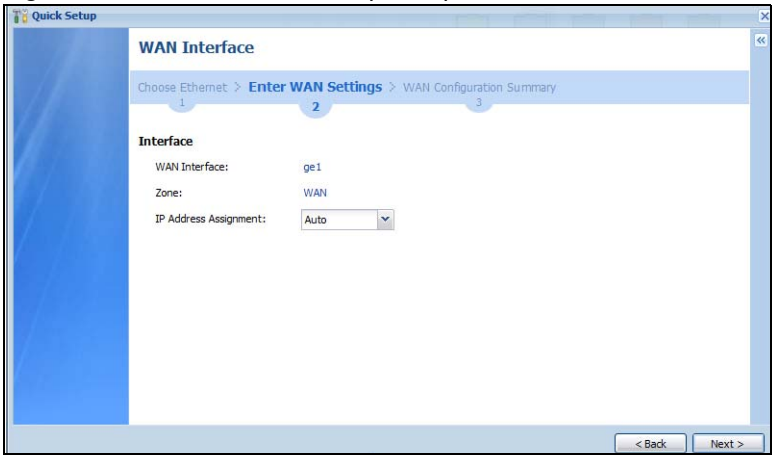
The screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

4.2.3 Configure WAN Settings

Use this screen to select whether the interface should use a fixed or dynamic IP address.

Figure 26 WAN Interface Setup: Step 2



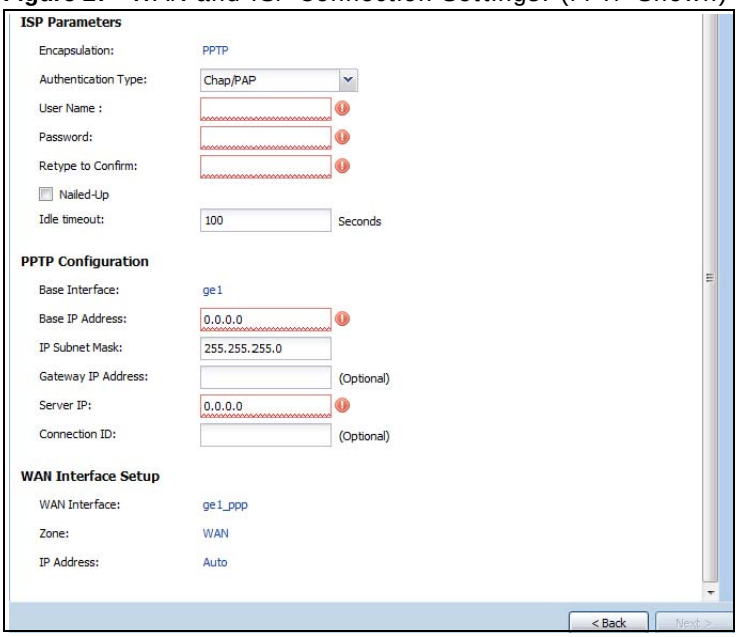
- **WAN Interface**: This is the interface you are configuring for Internet access.
- **Zone**: This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment**: Select **Auto** If your ISP did not assign you a fixed IP address. Select **Static** if you have a fixed IP address.

4.2.4 WAN and ISP Connection Settings

Use this screen to configure the ISP and WAN interface settings. This screen is read-only if you set the **IP Address Assignment** to **Static**.

Note: Enter the Internet access information exactly as your ISP gave it to you.

Figure 27 WAN and ISP Connection Settings: (PPTP Shown)



The following table describes the labels in this screen.

Table 12 WAN and ISP Connection Settings

LABEL	DESCRIPTION
ISP Parameter	This section appears if the interface uses a PPPoE or PPTP Internet connection.
Encapsulation	This displays the type of Internet connection you are configuring.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only. **MSCHAP** - Your ZyWALL accepts MSCHAP only. **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout.
PPTP Configuration	This section only appears if the interface uses a PPPoE or PPTP Internet connection.
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).

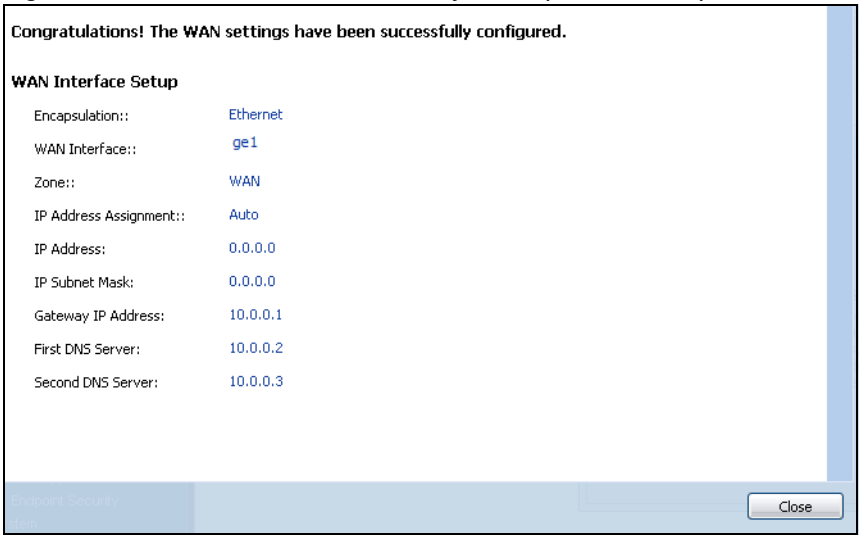
Table 12 WAN and ISP Connection Settings (continued)

LABEL	DESCRIPTION
Server IP	Type the IP address of the PPTP server.
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and -_: characters, and it can be up to 31 characters long.
WAN Interface Setup	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a static IP address, enter it in this field.
First DNS Server Second DNS Server	These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

4.2.5 Quick Setup Interface Wizard: Summary

This screen displays the WAN interface's settings.

Figure 28 Interface Wizard: Summary WAN (PPTP Shown)



The following table describes the labels in this screen.

Table 13 Interface Wizard: Summary WAN

LABEL	DESCRIPTION
Encapsulation	This displays what encapsulation this interface uses to connect to the Internet.
Service Name	This field only appears for a PPPoE interface. It displays the PPPoE service name specified in the ISP account.
Server IP	This field only appears for a PPTP interface. It displays the IP address of the PPTP server.
User Name	This is the user name given to you by your ISP.
Nailed-Up	If **No** displays the connection will not time out. **Yes** means the ZyWALL uses the idle timeout.
Idle Timeout	This is how many seconds the connection can be idle before the router automatically disconnects from the PPPoE server. 0 means no timeout.
Connection ID	If you specified a connection ID, it displays here.
WAN Interface	This identifies the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address Assignment	This field displays whether the WAN IP address is static or dynamic (**Auto**).
First DNS Server Second DNS Server	If the **IP Address Assignment** is **Static**, these fields display the DNS server IP address(es).
Close	Click **Close** to exit the wizard.

4.3 VPN Setup Wizard

Click **VPN Setup** in the main **Quick Setup** screen to open the VPN Setup Wizard **Welcome** screen.

Figure 29 VPN Setup Wizard

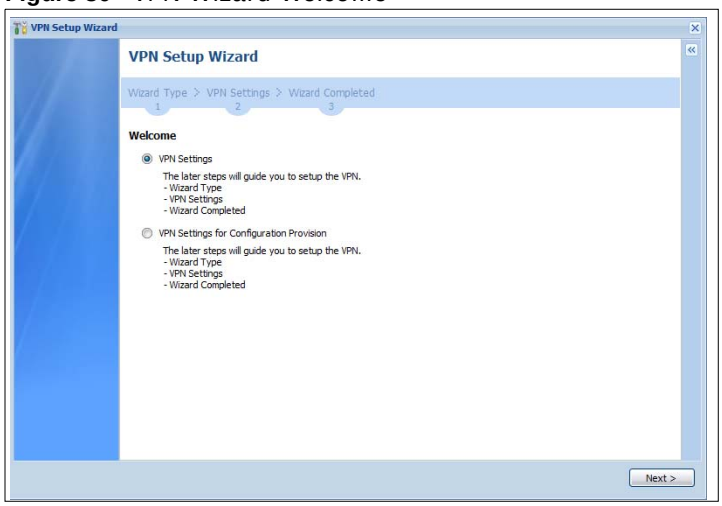

Quick Setup
WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.
VPN Setup
For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

4.3.1 Welcome

Use wizards to create Virtual Private Network (VPN) rules. After you complete the wizard, the Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen.

- **VPN Setup** configures a VPN tunnel for a secure connection to another computer or network.
- **VPN Settings for Configuration Provisioning** sets up a VPN rule the ZyWALL IPSec VPN Client can retrieve. Just enter a user name, password and the IP address of the ZyWALL in the ZyWALL IPSec VPN Client to get the VPN settings automatically from the ZyWALL.

Figure 30 VPN Wizard Welcome

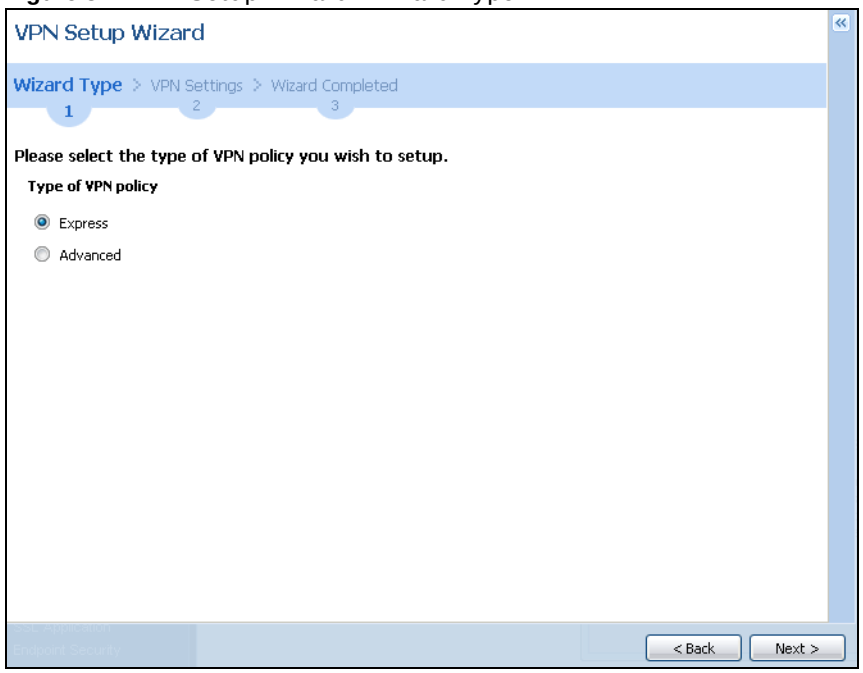


4.3.2 VPN Setup Wizard: Wizard Type

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings to connect to another ZLD-based ZyWALL using a pre-shared key.

Choose **Advanced** to change the default settings and/or use certificates instead of a pre-shared key to create a VPN rule to connect to another IPSec device.

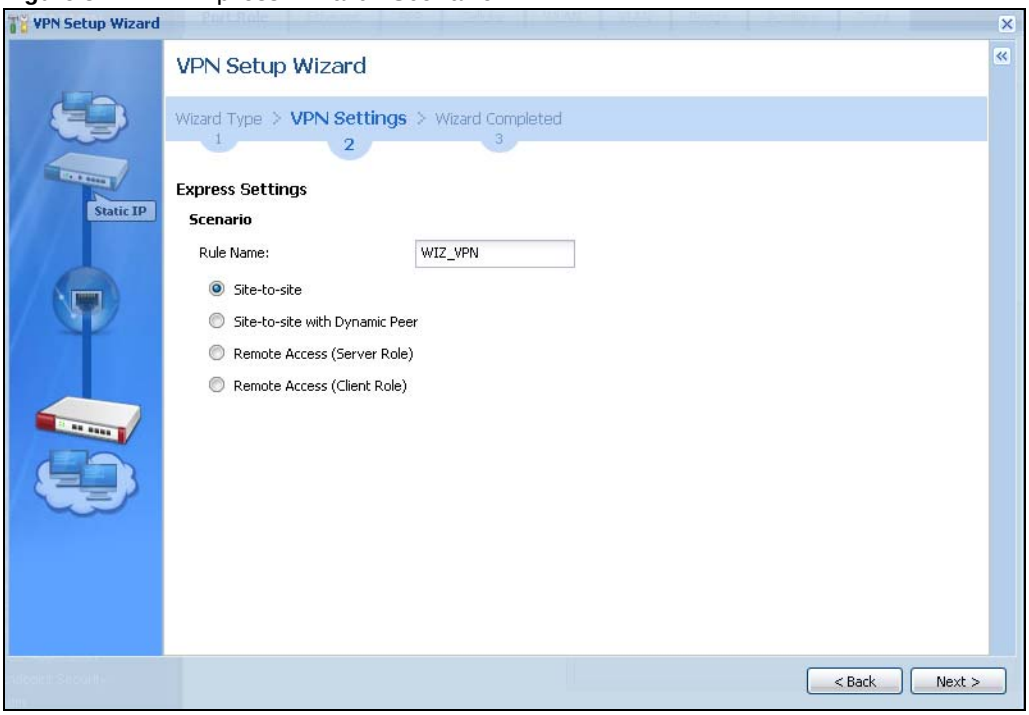
Figure 31 VPN Setup Wizard: Wizard Type



4.3.3 VPN Express Wizard - Scenario

Click the **Express** radio button as shown in Figure 31 on page 49 to display the following screen.

Figure 32 VPN Express Wizard: Scenario



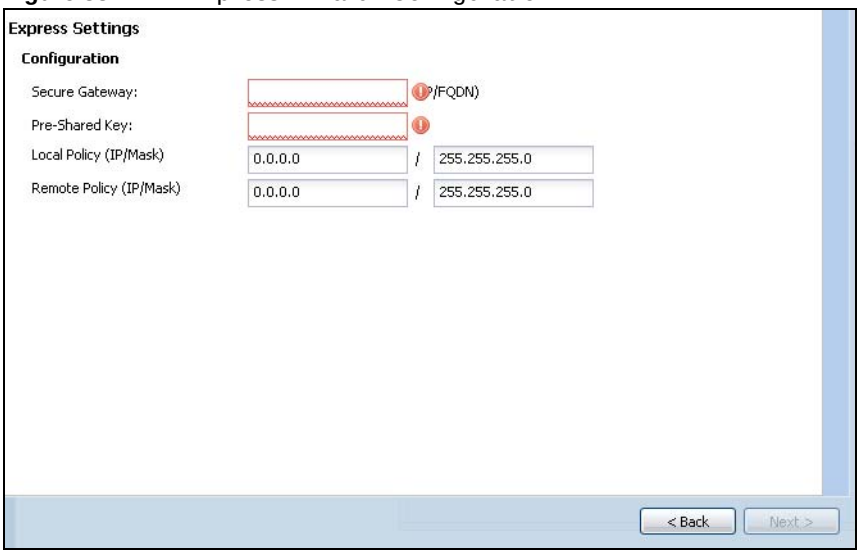
Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- **Site-to-site** - The remote IPSec device has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel.
- **Site-to-site with Dynamic Peer** - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- **Remote Access (Server Role)** - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- **Remote Access (Client Role)** - Connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel.

4.3.4 VPN Express Wizard - Configuration

Figure 33 VPN Express Wizard: Configuration

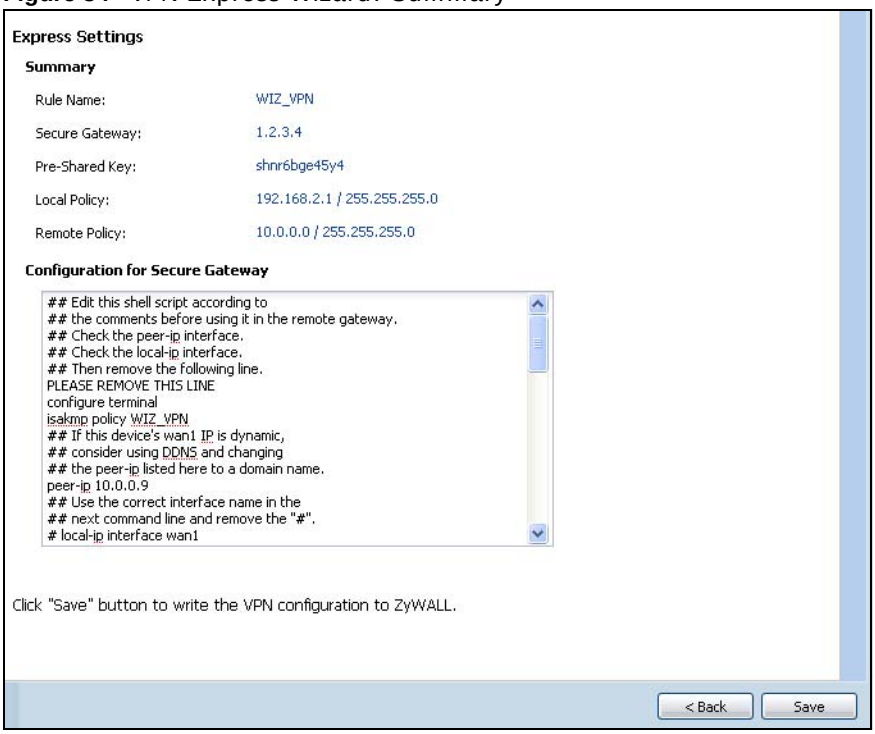


- **Secure Gateway**: **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.
- **Pre-Shared Key**: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.

4.3.5 VPN Express Wizard - Summary

This screen provides a read-only summary of the VPN tunnel's configuration and commands that you can copy and paste into another ZLD-based ZyWALL's command line interface to configure it.

Figure 34 VPN Express Wizard: Summary

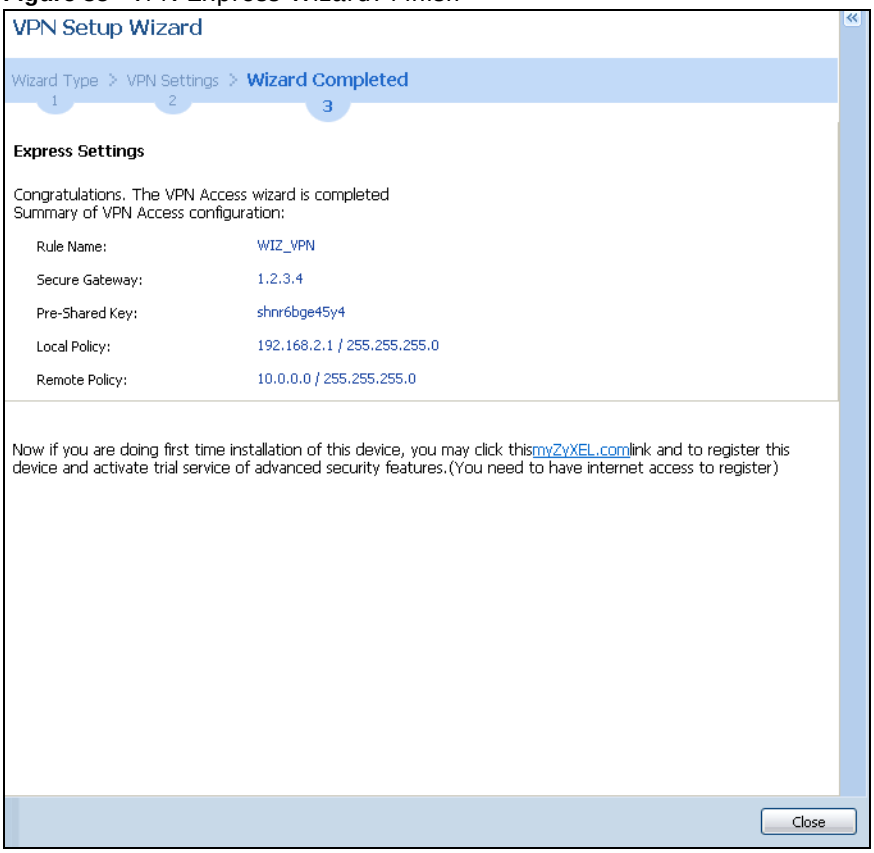

Express Settings
Summary
Rule Name:
WIZ_VPN
Secure Gateway:
1.2.3.4
Pre-Shared Key:
shnr6bge45y4
Local Policy:
192.168.2.1 / 255.255.255.0
Remote Policy:
10.0.0.0 / 255.255.255.0
Configuration for Secure Gateway
Edit this shell script according to
the comments before using it in the remote gateway.
Check the peer-ip interface.
Check the local-ip interface.
Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN
If this device's wan1 IP is dynamic,
consider using DDNS and changing
the peer-ip listed here to a domain name.
peer-ip 10.0.0.9
Use the correct interface name in the
next command line and remove the "#".
local-ip interface wan1
Click "Save" button to write the VPN configuration to ZyWALL.
< Back
Save

- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: IP address or domain name of the remote IPSec device. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.
- **Remote Policy**: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- Copy and paste the **Configuration for Secure Gateway** commands into another ZLD-based ZyWALL's command line interface to configure it to serve as the other end of this VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.

4.3.6 VPN Express Wizard - Finish

Now the rule is configured on the ZyWALL. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen.

Figure 35 VPN Express Wizard: Finish

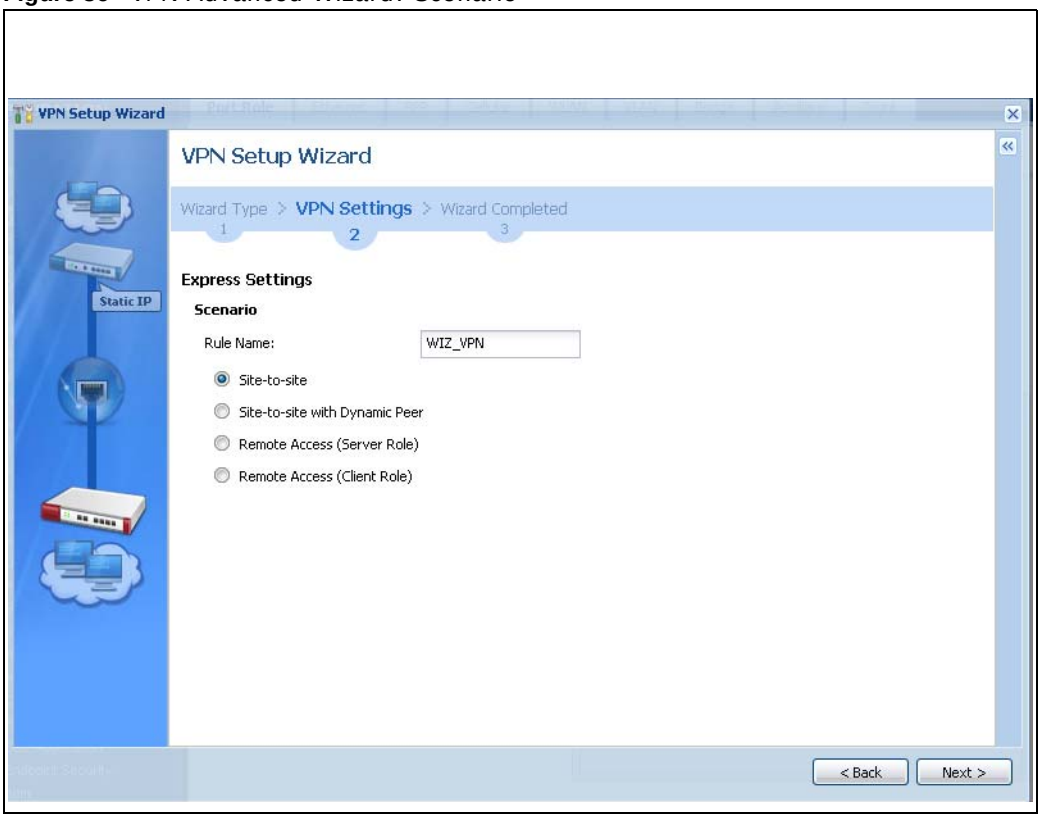

VPN Setup Wizard
Wizard Type > VPN Settings > Wizard Completed
1
2
3
Express Settings
Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:
Rule Name: WIZ_VPN
Secure Gateway: 1.2.3.4
Pre-Shared Key: shnr6bge45y4
Local Policy: 192.168.2.1 / 255.255.255.0
Remote Policy: 10.0.0.0 / 255.255.255.0
Now if you are doing first time installation of this device, you may click thismyZyXEL.comlink and to register this device and activate trial service of advanced security features.(You need to have internet access to register)
Close

Click **Close** to exit the wizard.

4.3.7 VPN Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in Figure 31 on page 49 to display the following screen.

Figure 36 VPN Advanced Wizard: Scenario



Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

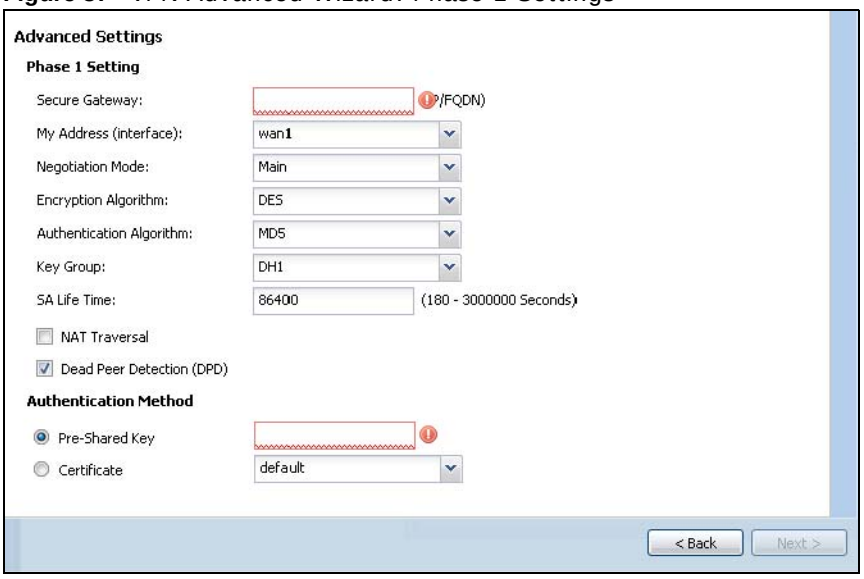
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- **Site-to-site** - The remote IPSec device has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel.
- **Site-to-site with Dynamic Peer** - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- **Remote Access (Server Role)** - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- **Remote Access (Client Role)** - Connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel.

4.3.8 VPN Advanced Wizard - Phase 1 Settings

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 37 VPN Advanced Wizard: Phase 1 Settings



- **Secure Gateway**: **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec device by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec device has a dynamic WAN IP address.
- **My Address (interface)**: Select an interface from the drop-down list box to use on your ZyWALL.
- **Negotiation Mode**: Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Note: Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key, and AES256 uses a 256-bit key.
- **Authentication Algorithm**: **MD5** gives minimal security and **SHA512** gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.
- **Key Group**: **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number.
- **SA Life Time**: Set how often the ZyWALL renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **NAT Traversal**: Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).

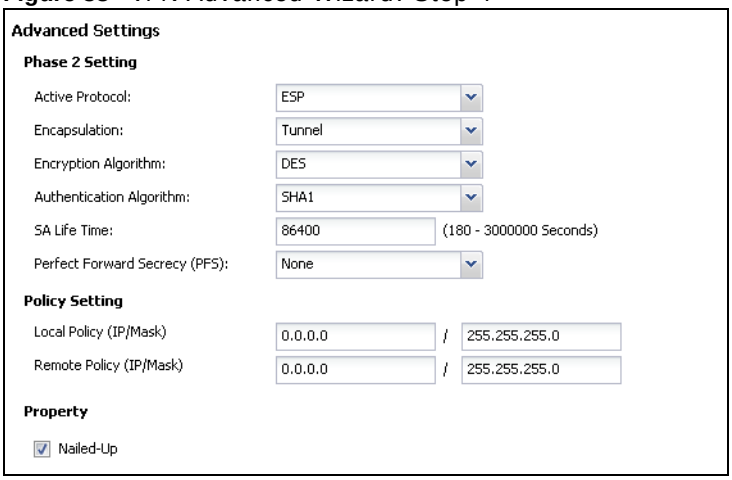
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- **Dead Peer Detection (DPD)** has the ZyWALL make sure the remote IPSec device is there before transmitting data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec device. If it responds, the ZyWALL transmits the data. If it does not respond, the ZyWALL shuts down the IKE SA.
- **Authentication Method**: Select **Pre-Shared Key** to use a password or **Certificate** to use one of the ZyWALL's certificates.

4.3.9 VPN Advanced Wizard - Phase 2

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Figure 38 VPN Advanced Wizard: Step 4

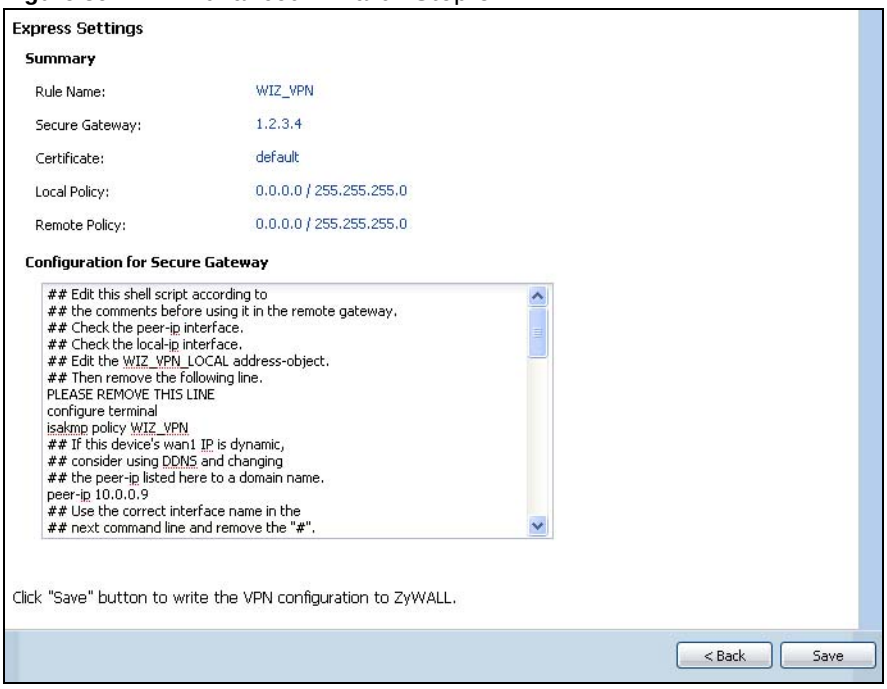


- **Active Protocol**: **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm**: **MD5** gives minimal security and **SHA512** gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.
- **SA Life Time**: Set how often the ZyWALL renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **Perfect Forward Secrecy (PFS)**: Disabling PFS allows faster IPSec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.
- **Nailed-Up**: This displays for the site-to-site and remote access client role scenarios. Select this to have the ZyWALL automatically renegotiate the IPSec SA when the SA life time expires.

4.3.10 VPN Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 39 VPN Advanced Wizard: Step 5

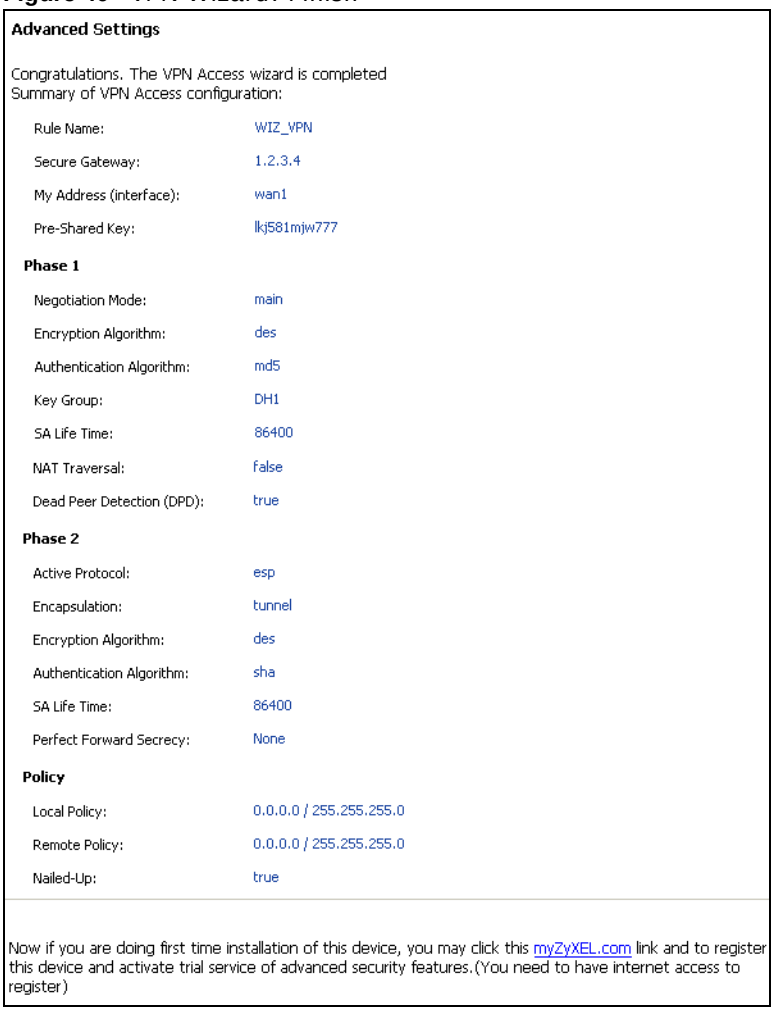

Express Settings
Summary
Rule Name:
WIZ_VPN
Secure Gateway:
1.2.3.4
Certificate:
default
Local Policy:
0.0.0.0 / 255.255.255.0
Remote Policy:
0.0.0.0 / 255.255.255.0
Configuration for Secure Gateway
Edit this shell script according to
the comments before using it in the remote gateway.
Check the peer-ip interface.
Check the local-ip interface.
Edit the WIZ_VPN_LOCAL address-object.
Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN
If this device's wan1 IP is dynamic,
consider using DDNS and changing
the peer-ip listed here to a domain name.
peer-ip 10.0.0.9
Use the correct interface name in the
next command line and remove the "#".
Click "Save" button to write the VPN configuration to ZyWALL.
< Back
Save

- **Rule Name**: Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway**: IP address or domain name of the remote IPSec device.
- **Pre-Shared Key**: VPN tunnel password.
- **Certificate**: The certificate the ZyWALL uses to identify itself when setting up the VPN tunnel.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.
- **Remote Policy**: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel.
- Copy and paste the **Configuration for Remote Gateway** commands into another ZLD-based ZyWALL's command line interface.
- Click **Save** to save the VPN rule.

4.3.11 VPN Advanced Wizard - Finish

Now the rule is configured on the ZyWALL. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN** Gateway screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen.

Figure 40 VPN Wizard: Finish


Advanced Settings
Congratulations. The VPN Access wizard is completed
Summary of VPN Access configuration:
Rule Name: WIZ_VPN
Secure Gateway: 1.2.3.4
My Address (interface): wan1
Pre-Shared Key: lkj581mjw777
Phase 1
Negotiation Mode: main
Encryption Algorithm: des
Authentication Algorithm: md5
Key Group: DH1
SA Life Time: 86400
NAT Traversal: false
Dead Peer Detection (DPD): true
Phase 2
Active Protocol: esp
Encapsulation: tunnel
Encryption Algorithm: des
Authentication Algorithm: sha
SA Life Time: 86400
Perfect Forward Secrecy: None
Policy
Local Policy: 0.0.0.0 / 255.255.255.0
Remote Policy: 0.0.0.0 / 255.255.255.0
Nailed-Up: true
Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

Click **Close** to exit the wizard.

4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type

Use VPN Settings for Configuration Provisioning to set up a VPN rule that can be retrieved with the ZyWALL IPSec VPN Client.

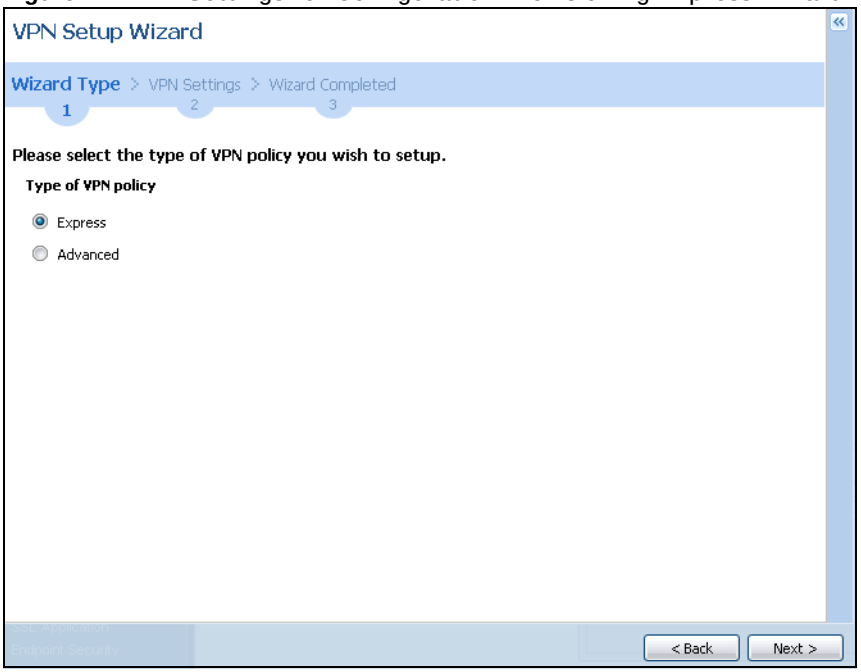
VPN rules for the ZyWALL IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- **AH** active protocol
- **NULL** encryption
- **SHA512** authentication
- A subnet or range remote policy

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key.

Choose **Advanced** to change the default settings and/or use certificates instead of a pre-shared key in the VPN rule.

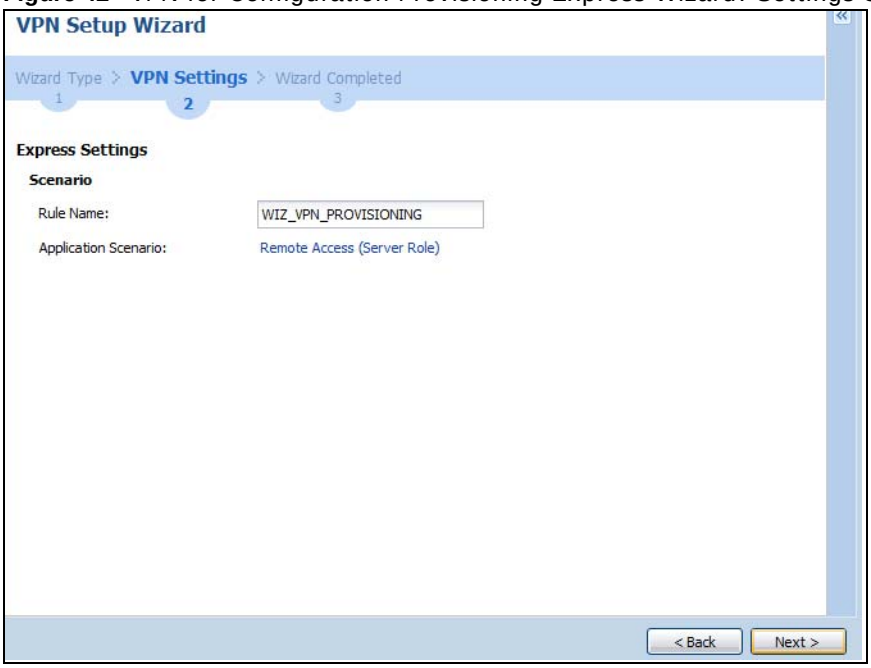
Figure 41 VPN Settings for Configuration Provisioning Express Wizard: Wizard Type



4.4.1 Configuration Provisioning Express Wizard - VPN Settings

Click the **Express** radio button as shown in the previous screen to display the following screen.

Figure 42 VPN for Configuration Provisioning Express Wizard: Settings Scenario



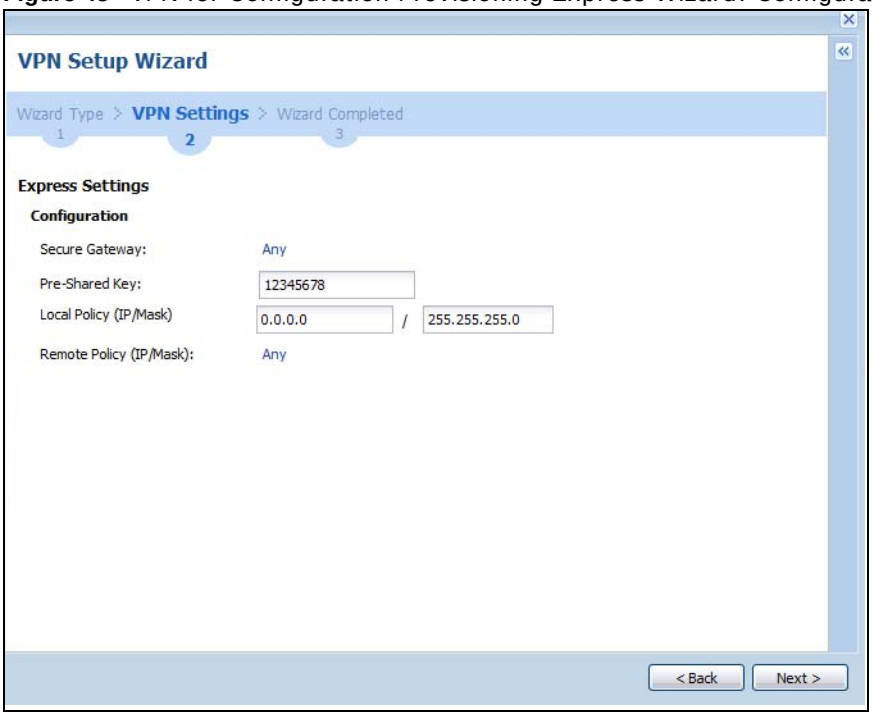
Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Application Scenario: Only the **Remote Access (Server Role)** is allowed in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.

4.4.2 Configuration Provisioning VPN Express Wizard - Configuration

Click **Next** to continue the wizard.

Figure 43 VPN for Configuration Provisioning Express Wizard: Configuration

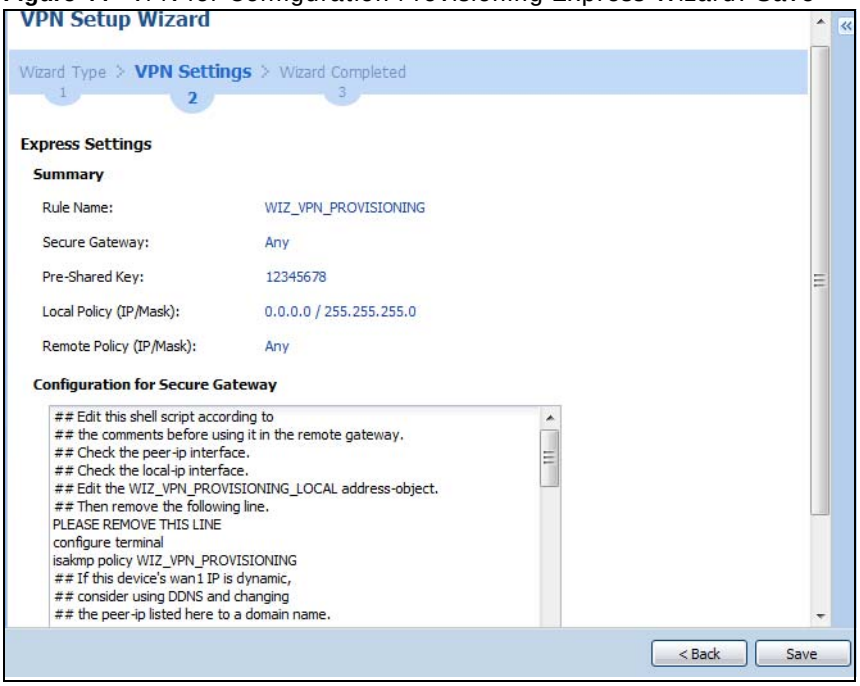


- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.
- **Pre-Shared Key**: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: **Any** displays in this field because it is not configurable in this wizard.

4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary

This screen has a read-only summary of the VPN tunnel's configuration and commands you can copy and paste into another ZLD-based ZyWALL's command line interface to configure it.

Figure 44 VPN for Configuration Provisioning Express Wizard: Save

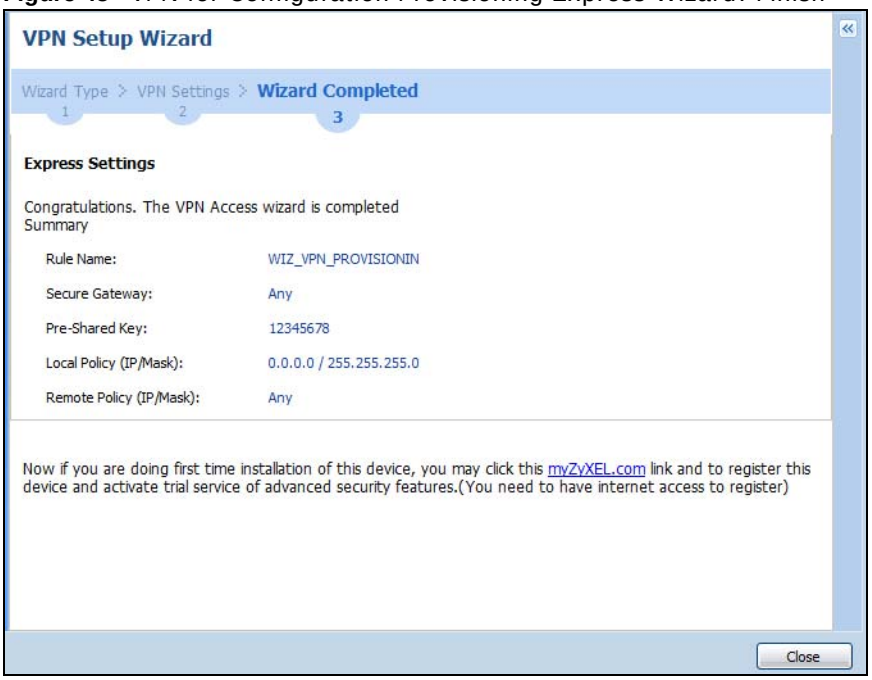

VPN Setup Wizard
Wizard Type > VPN Settings > Wizard Completed
1
2
3
Express Settings
Summary
Rule Name: WIZ_VPN_PROVISIONING
Secure Gateway: Any
Pre-Shared Key: 12345678
Local Policy (IP/Mask): 0.0.0.0 / 255.255.255.0
Remote Policy (IP/Mask): Any
Configuration for Secure Gateway
Edit this shell script according to
the comments before using it in the remote gateway.
Check the peer-ip interface.
Check the local-ip interface.
Edit the WIZ_VPN_PROVISIONING_LOCAL address-object.
Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN_PROVISIONING
If this device's wan1 IP is dynamic,
consider using DDNS and changing
the peer-ip listed here to a domain name.
< Back
Save

- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: (Static) IP address and subnet mask of the computers on the network behind your ZyWALL that can be accessed using the tunnel.
- **Remote Policy**: **Any** displays in this field because it is not configurable in this wizard.
- The **Configuration for Secure Gateway** displays the configuration that the ZyWALL IPSec VPN Client will get from the ZyWALL.

4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish

Now the rule is configured on the ZyWALL. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Enter the IP address of the ZyWALL in the ZyWALL IPSec VPN Client to get all these VPN settings automatically from the ZyWALL.

Figure 45 VPN for Configuration Provisioning Express Wizard: Finish

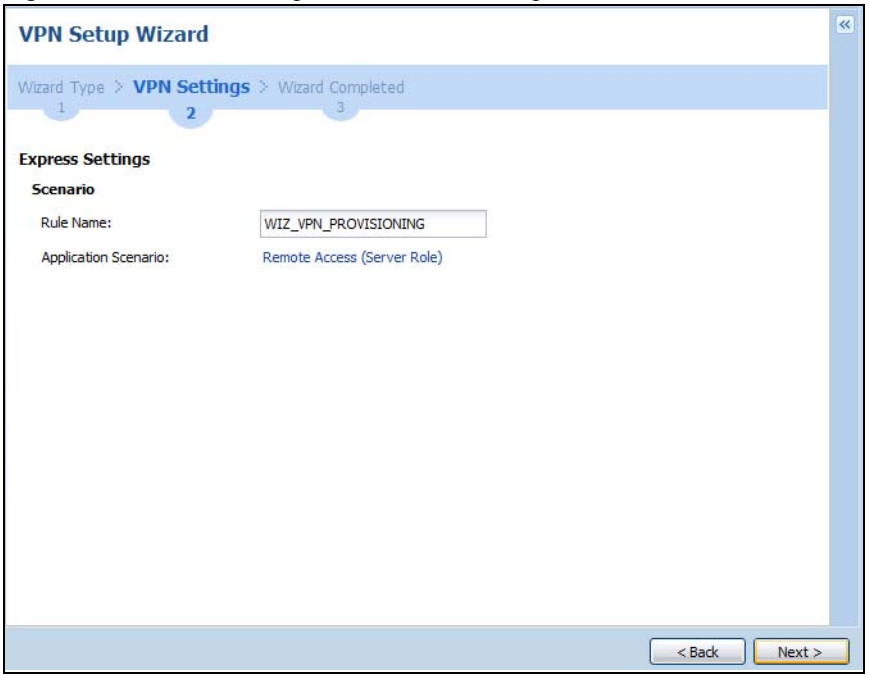

VPN Setup Wizard
Wizard Type > VPN Settings > Wizard Completed
1
2
3
Express Settings
Congratulations. The VPN Access wizard is completed
Summary
Rule Name:
WIZ_VPN_PROVISIONIN
Secure Gateway:
Any
Pre-Shared Key:
12345678
Local Policy (IP/Mask):
0.0.0.0 / 255.255.255.0
Remote Policy (IP/Mask):
Any
Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)
Close

Click **Close** to exit the wizard.

4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in the screen shown in Figure 41 on page 59 to display the following screen.

Figure 46 VPN for Configuration Provisioning Advanced Wizard: Scenario Settings



Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

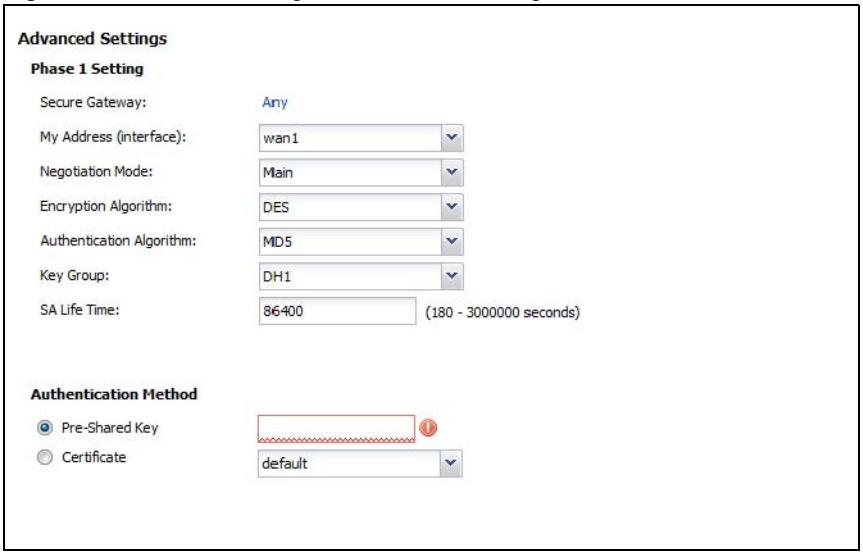
Application Scenario: Only the **Remote Access (Server Role)** is allowed in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.

Click **Next** to continue the wizard.

4.4.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 47 VPN for Configuration Provisioning Advanced Wizard: Phase 1 Settings



- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.
- **My Address (interface)**: Select an interface from the drop-down list box to use on your ZyWALL.
- **Negotiation Mode**: Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Note: Multiple SAs connecting through a secure gateway must have the same negotiation mode.

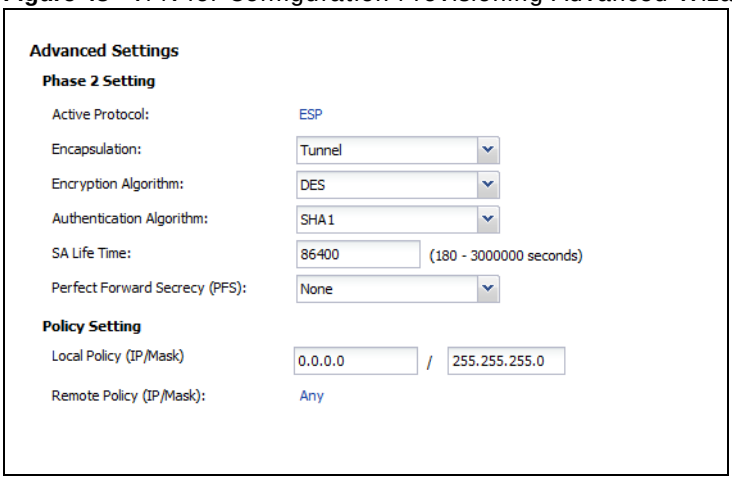
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key and AES256 uses a 256-bit key.

- **Authentication Algorithm**: MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. **MD5** gives minimal security. **SHA1** gives higher security and **SHA256** gives the highest security. The stronger the algorithm, the slower it is.
- **Key Group**: **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number.
- **SA Life Time**: Set how often the ZyWALL renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **Authentication Method**: Select **Pre-Shared Key** to use a password or **Certificate** to use one of the ZyWALL's certificates.

4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPSec.

Figure 48 VPN for Configuration Provisioning Advanced Wizard: Phase 2



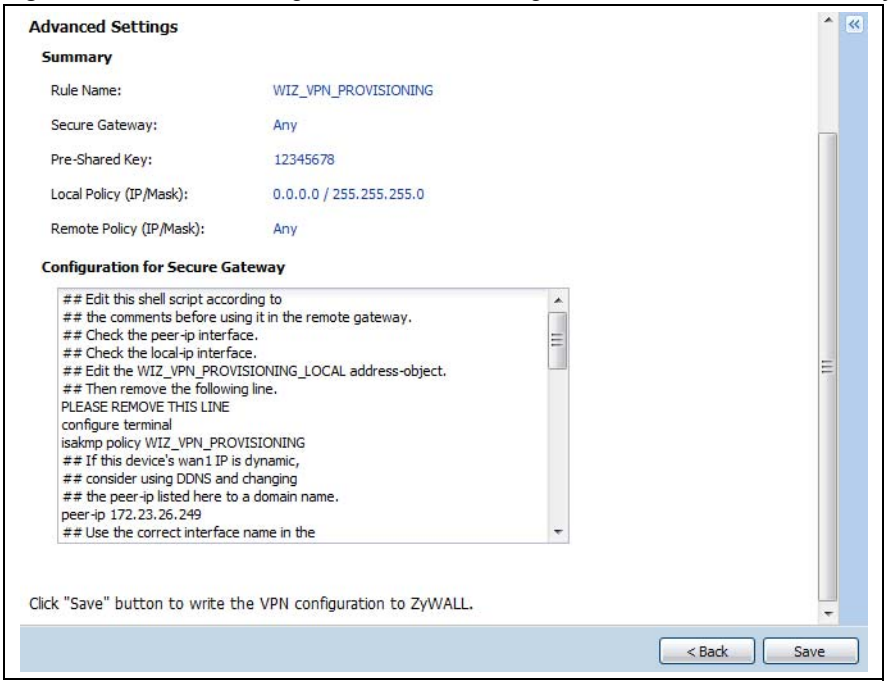
- **Active Protocol**: **ESP** is compatible with NAT. **AH** is not available in this wizard.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm**: MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. **MD5** gives minimal security. **SHA1** gives higher security and **SHA256** gives the highest security. The stronger the algorithm, the slower it is.
- **SA Life Time**: Set how often the ZyWALL renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **Perfect Forward Secrecy (PFS):** Disabling PFS allows faster IPSec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- **Local Policy (IP/Mask)**: Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.

- **Remote Policy (IP/Mask)**: **Any** displays in this field because it is not configurable in this wizard.
- **Nailed-Up**: This displays for the site-to-site and remote access client role scenarios. Select this to have the ZyWALL automatically renegotiate the IPSec SA when the SA life time expires.

4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 49 VPN for Configuration Provisioning Advanced Wizard: Summary


Advanced Settings
Summary
Rule Name:
WIZ_VPN_PROVISIONING
Secure Gateway:
Any
Pre-Shared Key:
12345678
Local Policy (IP/Mask):
0.0.0.0 / 255.255.255.0
Remote Policy (IP/Mask):
Any
Configuration for Secure Gateway
Edit this shell script according to
the comments before using it in the remote gateway.
Check the peer-ip interface.
Check the local-ip interface.
Edit the WIZ_VPN_PROVISIONING_LOCAL address-object.
Then remove the following line.
PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN_PROVISIONING
If this device's wan1 IP is dynamic,
consider using DDNS and changing
the peer-ip listed here to a domain name.
peer-ip 172.23.26.249
Use the correct interface name in the
Click "Save" button to write the VPN configuration to ZyWALL.
< Back
Save

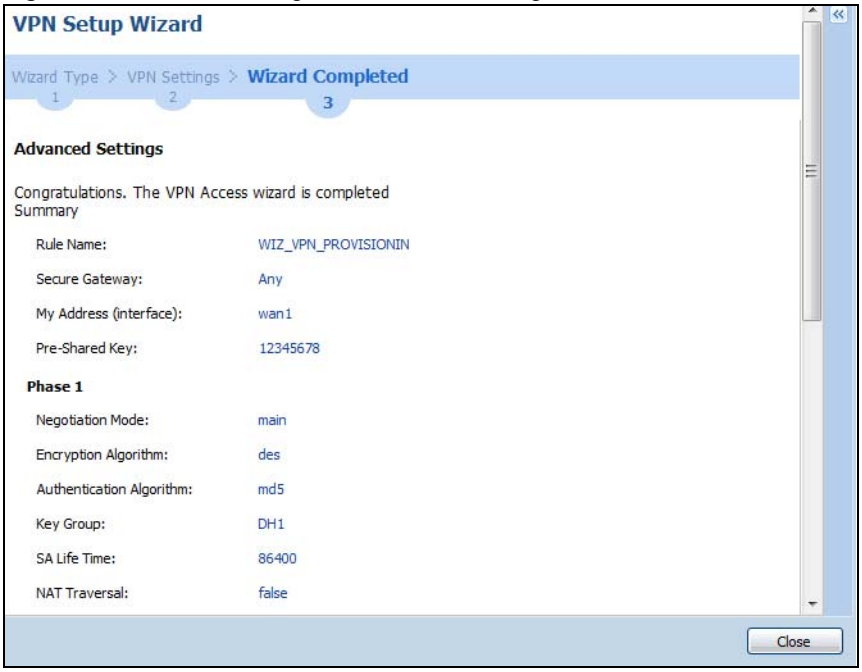
- **Rule Name**: Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the ZyWALL IPSec VPN Client.
- **Pre-Shared Key**: VPN tunnel password.
- **Certificate**: The certificate the ZyWALL uses to identify itself when setting up the VPN tunnel.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.
- **Remote Policy**: **Any** displays in this field because it is not configurable in this wizard.
- The **Configuration for Secure Gateway** displays the configuration that the ZyWALL IPSec VPN Client will get from the ZyWALL.
- Click **Save** to save the VPN rule.

4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish

Now the rule is configured on the ZyWALL. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN** Gateway screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN >**

VPN Connection screen. Enter the IP address of the ZyWALL in the ZyWALL IPSec VPN Client to get all these VPN settings automatically from the ZyWALL.

Figure 50 VPN for Configuration Provisioning Advanced Wizard: Finish



Click **Close** to exit the wizard.

5

Dashboard

5.1 Overview

Use the **Dashboard** screens to check status information about the ZyWALL.

5.1.1 What You Can Do in this Chapter

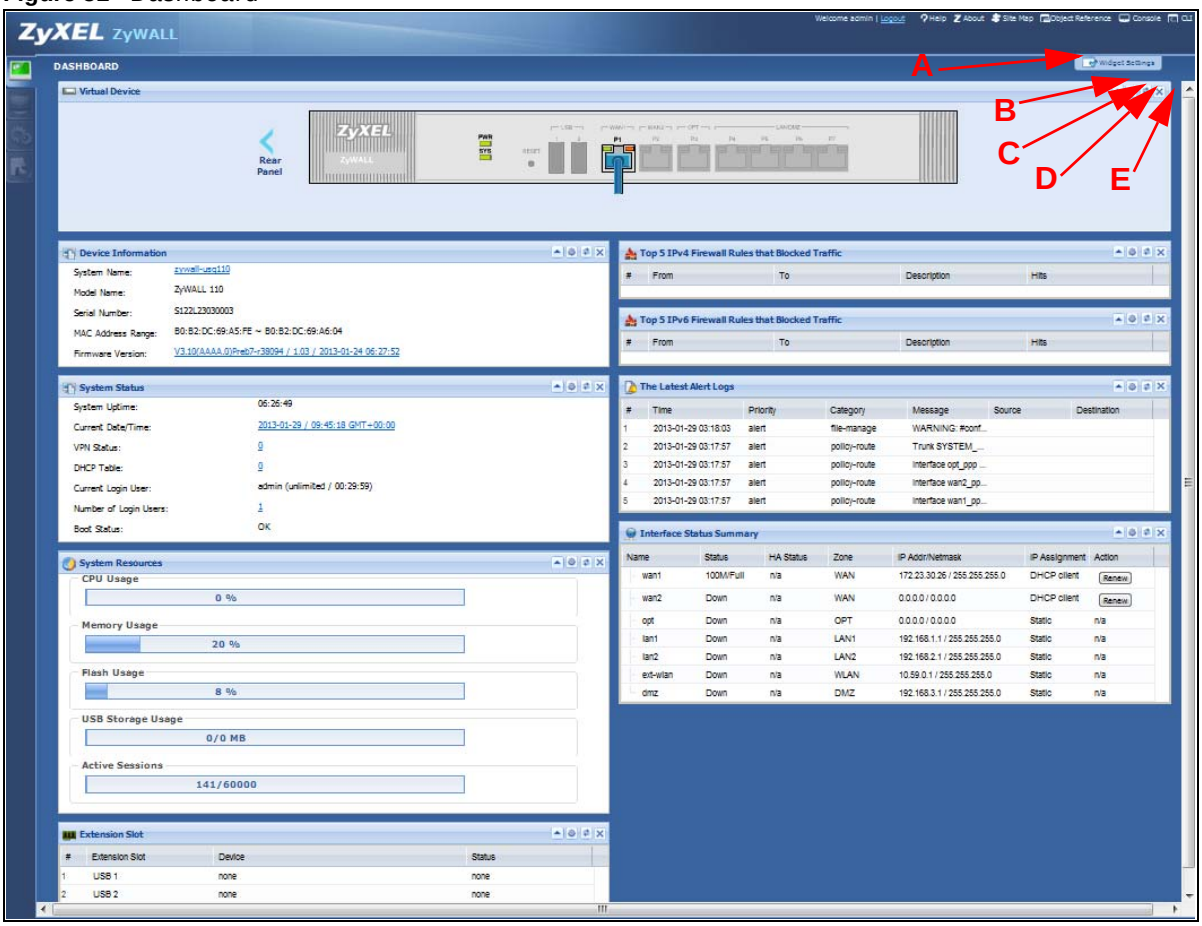
Use the **Dashboard** screens for the following.

- Use the main **Dashboard** screen (see Section 5.2 on page 69) to see the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status. You can also display other status screens for more information.
- Use the **VPN** status screen (see Section 5.2.4 on page 76) to look at the VPN tunnels that are currently established.
- Use the **DHCP Table** screen (see Section 5.2.5 on page 77) to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
- Use the **Current Users** screen (see Section 5.2.6 on page 78) to look at a list of the users currently logged into the ZyWALL.

5.2 The Dashboard Screen

The **Dashboard** screen displays when you log into the ZyWALL or click **Dashboard** in the navigation panel. The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 51 Dashboard



The following table describes the labels in this screen.

Table 14 Dashboard

LABEL	DESCRIPTION
Widget Setting (A)	Use this link to open or close widgets by selecting/clearing the associated checkbox.
Up Arrow (B)	Click this to collapse a widget. It then becomes a down arrow. Click it again to enlarge the widget again.
Refresh Time Setting (C)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (D)	Click this to update the widget's information immediately.
Close Widget (E)	Click this to close the widget. Use **Widget Setting** to re-open it.
Virtual Device	
Rear Panel	Click this to view details about the ZyWALL's rear panel. Hover your cursor over a connected interface or slot to display status details.
Front Panel	Click this to view details about the status of the ZyWALL's front panel LEDs and connections. See Section 3.5 on page 39 for LED descriptions. An unconnected interface or slot appears grayed out.
	The following front and rear panel labels display when you hover your cursor over a connected interface or slot.
Name	This field displays the name of each interface.
Slot	This field displays the name of each extension slot.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Device	This field displays the name of the device connected to the USB port if one is connected.
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 7.5 on page 132 the Web Help for the status that can appear.
Zone	This field displays the zone to which the interface is currently assigned.
IP Address/ Mask	This field displays the current IP address and subnet mask assigned to the interface. If the interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
Device Information	This identifies a device installed in one of the ZyWALL's extension slots or USB ports.
System Name	This field displays the name used to identify the ZyWALL on any network. Click the icon to open the screen where you can change it.
Model Name	This field displays the model name of this ZyWALL.
Serial Number	This field displays the serial number of this ZyWALL. The serial number is used for device tracking and control.
MAC Address Range	This field displays the MAC addresses used by the ZyWALL. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the ZyWALL is currently running. Click the icon to open the screen where you can upload firmware.
System Status	
System Uptime	This field displays how long the ZyWALL has been running since it last restarted or was turned on.
Current Date/Time	This field displays the current date and time in the ZyWALL. The format is yyyy-mm-dd hh:mm:ss.
VPN Status	Click this to look at the VPN tunnels that are currently established. See Section 5.2.1 on page 74.
DHCP Table	Click this to look at the IP addresses currently assigned to the ZyWALL's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 5.2.5 on page 77.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.
Number of Login Users	This field displays the number of users currently logged in to the ZyWALL. Click the icon to pop-open a list of the users who are currently logged in to the ZyWALL.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Boot Status	This field displays details about the ZyWALL's startup state. **OK** - The ZyWALL started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The ZyWALL successfully applied the system default configuration. This occurs when the ZyWALL starts for the first time or you intentionally reset the ZyWALL to the system default settings. **Fallback to lastgood configuration** - The ZyWALL was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The ZyWALL was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The ZyWALL is still applying the system configuration.
System Resources	
CPU Usage	This field displays what percentage of the ZyWALL's processing capability is currently being used. Hover your cursor over this field to display the **Show CPU Usage** icon that takes you to a chart of the ZyWALL's recent CPU usage.
Memory Usage	This field displays what percentage of the ZyWALL's RAM is currently being used. Hover your cursor over this field to display the **Show Memory Usage** icon that takes you to a chart of the ZyWALL's recent memory usage.
Flash Usage	This field displays what percentage of the ZyWALL's onboard flash memory is currently being used.
USB Storage Usage	This field shows how much storage in the USB device connected to the ZyWALL is in use.
Active Sessions	This field shows how many sessions, established and non-established, that pass through/from/to/within the ZyWALL. Hover your cursor over this field to display icons. Click the **Detail** icon to go to the **Session Monitor** screen to see details about the active sessions. Click the **Show Active Sessions** icon to display a chart of ZyWALL's recent session usage.
Extension Slot	This section of the screen displays the status of the extension card slot the USB ports.
Extension Slot	This field displays the name of each extension slot.
Device	This field displays the name of the device connected to the extension slot (or **none** if no device is detected). **USB Flash Drive** - Indicates a connected USB storage device and the drive's storage capacity.
Status	For cellular (3G) interfaces, see Section 6.10 on page 96 the Web Help for the status that can appear. Ready - A USB storage device connected to the ZyWALL is ready for the ZyWALL to use. **Unused** - The ZyWALL is unable to mount a USB storage device connected to the ZyWALL.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
#	This shows how many interfaces there are.
Name	This field displays the name of each interface.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For PPP interfaces: **Connected** - The PPP interface is connected. **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list.
Zone	This field displays the zone to which the interface is currently assigned.
IP Addr/ Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0/0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click the **Connect** icon to have the ZyWALL try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**. Click the **Disconnect** icon to stop a PPPoE/PPTP connection.
Top 5 Firewall Rules that blocked IPv4 (IPv6) Traffic	This section displays the most triggered five firewall rules that caused the ZyWALL to block .
#	This is the entry's rank in the list of the most commonly triggered firewall rules.
Priority	This is the position of the triggered firewall rule in the global rule list. The ordering of firewall rules is important as rules are applied in sequence.
From	This shows the zone packets came from that the triggered firewall rule.
To	This shows the zone packets went to that the triggered firewall rule.
Description	This field displays the descriptive name (if any) of the triggered firewall rule.
Hits	This field displays how many times the firewall rule was triggered.
Schedule	This field displays the schedule object of the triggered firewall rule.
User	This is the user name or user group name of the triggered firewall rule.
IPv4 (IPv6) Source	This displays the source IPv4 (IPv6) address object of the triggered firewall rule.
IPv4 (IPv6) Destination	This displays the destination IPv4 (IPv6) address object of the triggered firewall rule.
Service	This displays the service object of the triggered firewall rule.
Access	This field displays whether the triggered firewall rule denied (silently discarded) or rejected the passage of packets of the triggered firewall rule.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Logs	This field displays whether a log (and alert) was created for the triggered firewall rule.
The Latest Alert Logs	These fields display recent logs generated by the ZyWALL.
#	This is the entry's rank in the list of alert logs.
Time	This field displays the date and time the log was created.
Priority	This field displays the severity of the log.
Category	This field displays the type of log generated.
Message	This field displays the actual log message.
Source	This field displays the source address (if any) in the packet that generated the log.
Destination	This field displays the destination address (if any) in the packet that generated the log.
Protocol	This field displays the service protocol in the packet that generated the log.
Note	This field displays descriptive information (if any) of the log.

5.2.1 The CPU Usage Screen

Use this screen to look at a chart of the ZyWALL's recent CPU usage. To access this screen, click **CPU Usage** in the dashboard.

Figure 52 Dashboard > CPU Usage



The following table describes the labels in this screen.

Table 15 Dashboard > CPU Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of CPU usage.
	The x-axis shows the time period over which the CPU usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh	Click this to update the information in the window right away.

5.2.2 The Memory Usage Screen

Use this screen to look at a chart of the ZyWALL's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the dashboard.

Figure 53 Dashboard > Memory Usage



The following table describes the labels in this screen.

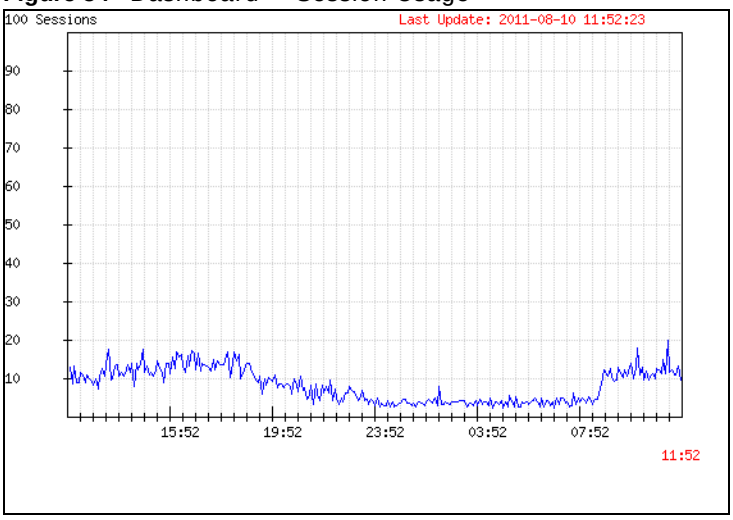
Table 16 Dashboard > Memory Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of RAM usage.
	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh	Click this to update the information in the window right away.

5.2.3 The Active Sessions Screen

Use this screen to look at a chart of the ZyWALL's recent traffic session usage. To access this screen, click **Session Usage** in the dashboard.

Figure 54 Dashboard > Session Usage



The following table describes the labels in this screen.

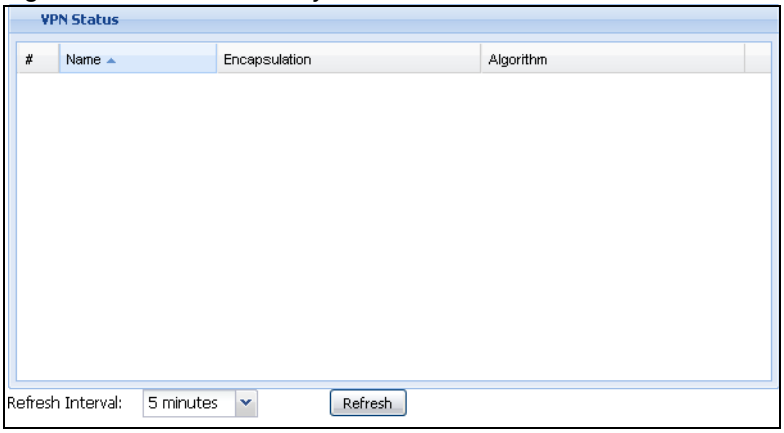
Table 17 Dashboard > Session Usage

LABEL	DESCRIPTION
Sessions	The y-axis represents the number of session.
	The x-axis shows the time period over which the session usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh	Click this to update the information in the window right away.

5.2.4 The VPN Status Screen

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in **System Status** in the dashboard.

Figure 55 Dashboard > System Status > VPN Status



The following table describes the labels in this screen.

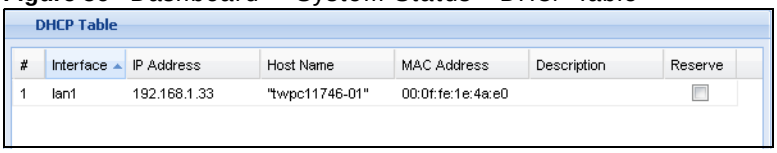
Table 18 Dashboard > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Refresh Interval	Select how often you want this window to be updated automatically.
Refresh	Click this to update the information in the window right away.

5.2.5 The DHCP Table Screen

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click **DHCP Table** in **System Status** in the dashboard.

Figure 56 Dashboard > System Status >DHCP Table


DHCP Table
Interface IP Address Host Name MAC Address Description Reserve
1 lan1 192.168.1.33 "twpc11746-01" 00:0f:fe:1e:4a:e0

The following table describes the labels in this screen.

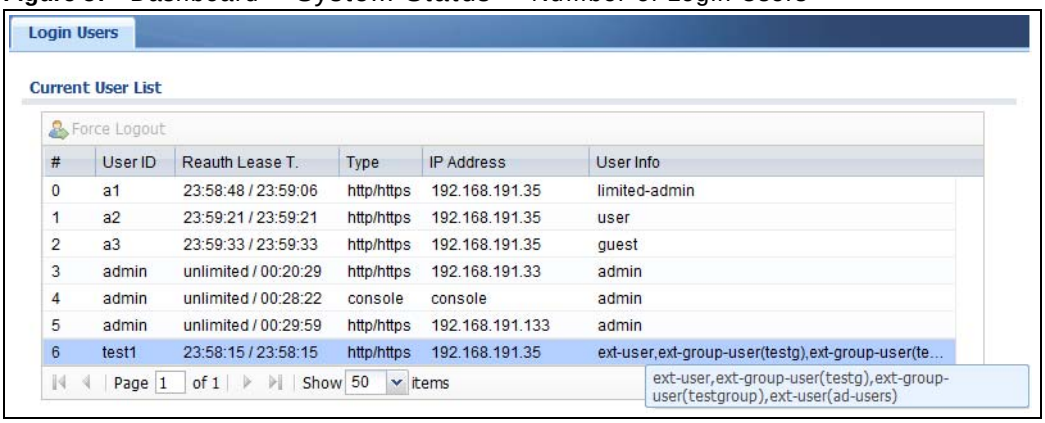
Table 19 Dashboard > DHCP Table

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests. "None" shows here for a static DHCP entry.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Reserve	If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address. If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client. To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click **Apply**. To remove a static DHCP entry, clear this field, and then click **Apply**.

5.2.6 The Number of Login Users Screen

Use this screen to look at a list of the users currently logged into the ZyWALL. Users who close their browsers without logging out are still shown as logged in here. To access this screen, click **Number of Login Users** in **System Status** in the dashboard or **Monitor > Login User.**

Figure 57 Dashboard > System Status > Number of Login Users


Login Users
Current User List
Force Logout
User ID Reauth Lease T. Type IP Address User Info
0 a1 23:58:48 / 23:59:06 http/https 192.168.191.35 limited-admin
1 a2 23:59:21 / 23:59:21 http/https 192.168.191.35 user
2 a3 23:59:33 / 23:59:33 http/https 192.168.191.35 guest
3 admin unlimited / 00:20:29 http/https 192.168.191.33 admin
4 admin unlimited / 00:28:22 console console admin
5 admin unlimited / 00:29:59 http/https 192.168.191.133 admin
6 test1 23:58:15 / 23:58:15 http/https 192.168.191.35 ext-user,ext-group-user(testg),ext-group-user(te...
Page 1 of 1 Show 50 items
ext-user,ext-group-user(testg),ext-group-user(testgroup),ext-user(ad-users)

The following table describes the labels in this screen.

Table 20 Dashboard > Number of Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ZyWALL.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 27 on page 371 for more information.
Type	This field displays the way the user logged in to the ZyWALL.
IP address	This field displays the IP address of the computer used to log in to the ZyWALL.
User Info	This field displays the types of user accounts the ZyWALL uses. If the user type is **ext-user** (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Force Logout	Click this icon to end a user's session.

6

Monitor

6.1 Overview

Use the **Monitor** screens to check status and statistics information.

6.1.1 What You Can Do in this Chapter

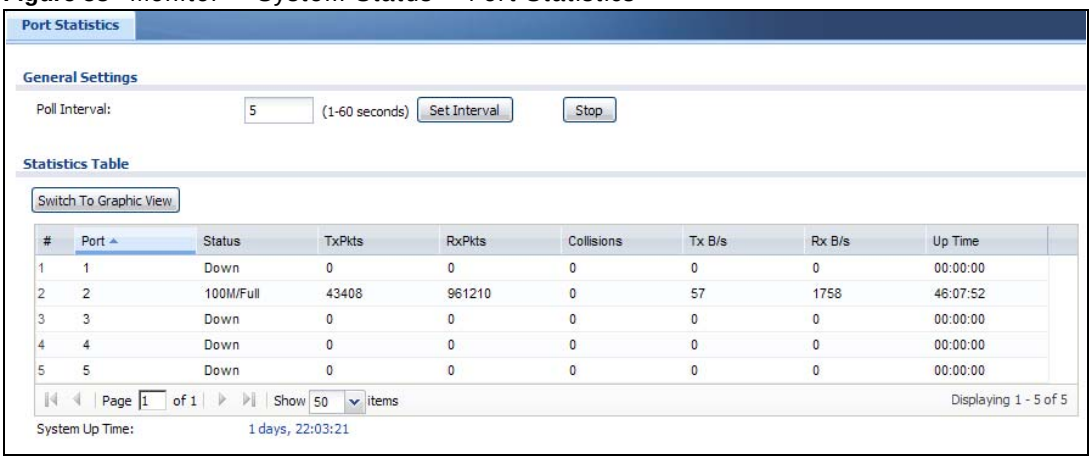
Use the **Monitor** screens for the following.

- Use the **System Status > Port Statistics** screen (see Section 6.2 on page 80) to look at packet statistics for each physical port.
- Use the **System Status > Port Statistics > Graph View** screen (see Section 6.2 on page 80) to look at a line graph of packet statistics for each physical port.
- Use the **System Status > Interface Status** screen (Section 6.3 on page 82) to see all of the ZyWALL's interfaces and their packet statistics.
- Use the **System Status > Traffic Statistics** screen (see Section 6.4 on page 86) to start or stop data collection and view statistics.
- Use the **System Status > Session Monitor** screen (see Section 6.5 on page 89) to view sessions by user or service.
- Use the **System Status > DDNS Status** screen (see Section 6.6 on page 91) to view the status of the ZyWALL's DDNS domain names.
- Use the **System Status > IP/MAC Binding** screen (Section 6.7 on page 91) to view a list of devices that have received an IP address from ZyWALL interfaces with IP/MAC binding enabled.
- Use the **System Status > Login Users** screen (Section 6.8 on page 92) to look at a list of the users currently logged into the ZyWALL.
- Use the **System Status > Cellular Status** screen (Section 6.9 on page 93) to check your 3G connection status.
- Use the **System Status > USB Storage** screen (Section 6.10 on page 96) to view information about a connected USB storage device.
- Use the **VPN Monitor** > **IPSec** screen (Section 6.11 on page 97) to display and manage active IPSec SAs.
- Use the **VPN Monitor > SSL** screen (see Section 6.12 on page 99) to list the users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
- Use the **VPN Monitor > L2TP over IPSec screen (see Section 6.13 on page 99) to display and manage the ZyWALL's connected L2TP VPN sessions.**
- Use the **Log** (Section 6.14 on page 100) screen to view the ZyWALL's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

6.2 The Port Statistics Screen

Use this screen to look at packet statistics for each Gigabit Ethernet port. To access this screen, click **Monitor > System Status** > **Port Statistics**.

Figure 58 Monitor > System Status > Port Statistics


Port Statistics
General Settings
Poll Interval:
5
(1-60 seconds)
Set Interval
Stop
Statistics Table
Switch To Graphic View
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
1 1 Down 0 0 0 0 0 00:00:00
2 2 100M/Full 43408 961210 0 57 1758 46:07:52
3 3 Down 0 0 0 0 0 00:00:00
4 4 Down 0 0 0 0 0 00:00:00
5 5 Down 0 0 0 0 0 00:00:00
Page 1 of 1
Show 50 items
Displaying 1 - 5 of 5
System Up Time:
1 days, 22:03:21

The following table describes the labels in this screen.

Table 21 Monitor > System Status > Port Statistics

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.
Switch to Graphic View	Click this to display the port statistics as a line graph.
#	This field displays the port's number in the list.
Port	This field displays the physical port number.
Status	This field displays the current status of the physical port. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the ZyWALL on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the ZyWALL on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the ZyWALL has been running since it last restarted or was turned on.

6.2.1 The Port Statistics Graph Screen

Use this screen to look at a line graph of packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen and then the **Switch to Graphic View Button**.

Figure 59 Monitor > System Status > Port Statistics > Switch to Graphic View



The following table describes the labels in this screen.

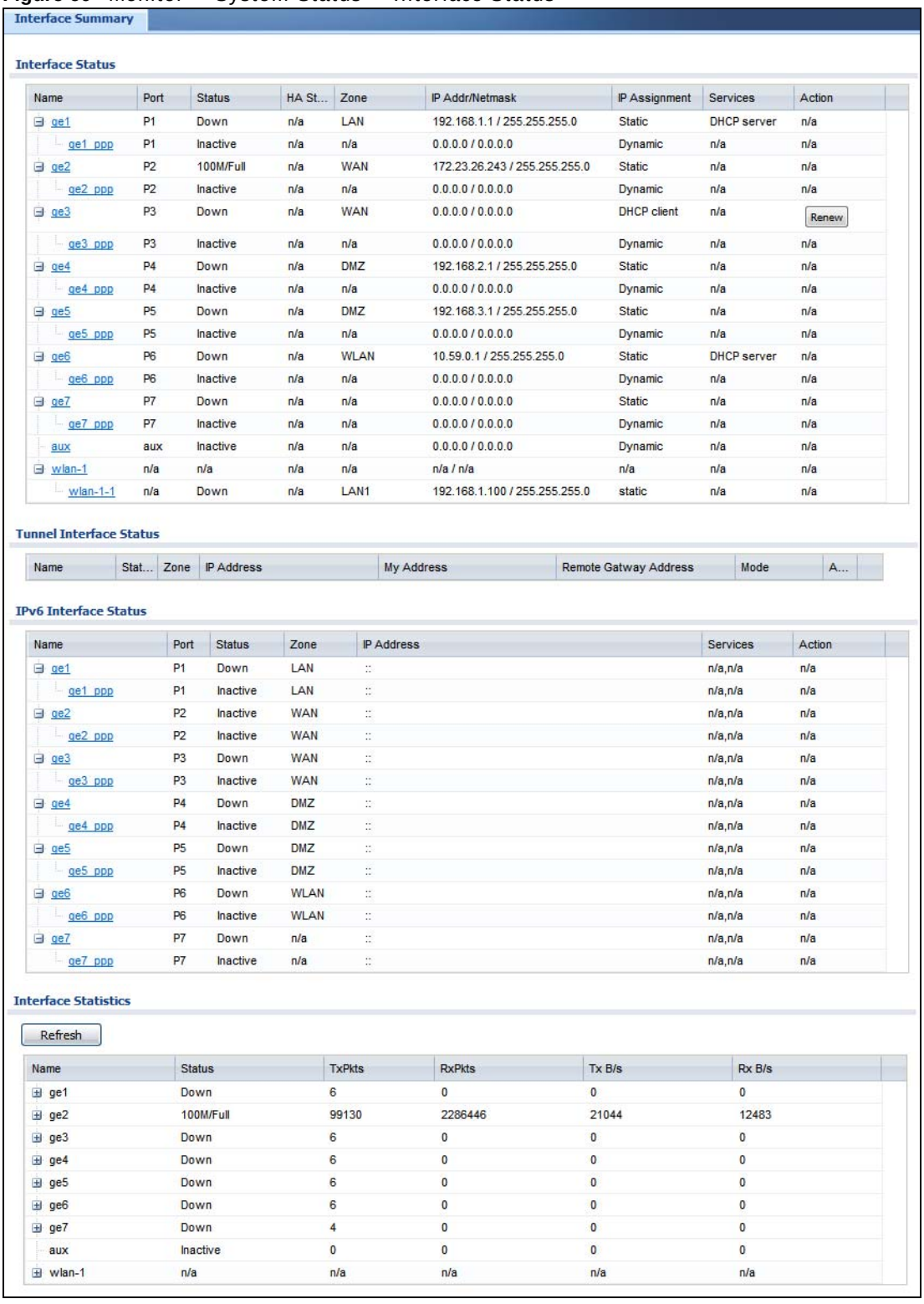
Table 22 Monitor > System Status > Port Statistics > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Selection	Select the number of the physical port for which you want to display graphics.
Switch to Grid View	Click this to display the port statistics as a table.
bps	The y-axis represents the speed of transmission or reception.
time	The x-axis shows the time period over which the transmission or reception occurred
TX	This line represents traffic transmitted from the ZyWALL on the physical port since it was last connected.
RX	This line represents the traffic received by the ZyWALL on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.
System Up Time	This field displays how long the ZyWALL has been running since it last restarted or was turned on.

6.3 Interface Status Screen

This screen lists all of the ZyWALL's interfaces and gives packet statistics for them. Click **Monitor > System Status > Interface Status** to access this screen.

Figure 60 Monitor > System Status > Interface Status



Interface Summary

Interface Status

Name	Port	Status	HA St...	Zone	IP Addr/Netmask	IP Assignment	Services	Action
ge1	P1	Down	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
ge1_ppp	P1	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge2	P2	100M/Full	n/a	WAN	172.23.26.243 / 255.255.255.0	Static	n/a	n/a
ge2_ppp	P2	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge3	P3	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
ge3_ppp	P3	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge4	P4	Down	n/a	DMZ	192.168.2.1 / 255.255.255.0	Static	n/a	n/a
ge4_ppp	P4	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge5	P5	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	n/a	n/a
ge5_ppp	P5	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge6	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
ge6_ppp	P6	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
ge7	P7	Down	n/a	n/a	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
ge7_ppp	P7	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
aux	aux	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	LAN1	192.168.1.100 / 255.255.255.0	static	n/a	n/a

Tunnel Interface Status

Name	Stat...	Zone	IP Address	My Address	Remote Gatway Address	Mode	A...

IPv6 Interface Status

Name	Port	Status	Zone	IP Address	Services	Action
ge1	P1	Down	LAN	::	n/a,n/a	n/a
ge1_ppp	P1	Inactive	LAN	::	n/a,n/a	n/a
ge2	P2	Inactive	WAN	::	n/a,n/a	n/a
ge2_ppp	P2	Inactive	WAN	::	n/a,n/a	n/a
ge3	P3	Down	WAN	::	n/a,n/a	n/a
ge3_ppp	P3	Inactive	WAN	::	n/a,n/a	n/a
ge4	P4	Down	DMZ	::	n/a,n/a	n/a
ge4_ppp	P4	Inactive	DMZ	::	n/a,n/a	n/a
ge5	P5	Down	DMZ	::	n/a,n/a	n/a
ge5_ppp	P5	Inactive	DMZ	::	n/a,n/a	n/a
ge6	P6	Down	WLAN	::	n/a,n/a	n/a
ge6_ppp	P6	Inactive	WLAN	::	n/a,n/a	n/a
ge7	P7	Down	n/a	::	n/a,n/a	n/a
ge7_ppp	P7	Inactive	n/a	::	n/a,n/a	n/a

Interface Statistics

Refresh

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	6	0	0	0
ge2	100M/Full	99130	2286446	21044	12483
ge3	Down	6	0	0	0
ge4	Down	6	0	0	0
ge5	Down	6	0	0	0
ge6	Down	6	0	0	0
ge7	Down	4	0	0	0
aux	Inactive	0	0	0	0
wlan-1	n/a	n/a	n/a	n/a	n/a

Each field is described in the following table.

Table 23 Monitor > System Status > Interface Status

LABEL	DESCRIPTION
Interface Status	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is an **Expand** icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.
Port	This field displays the physical port number.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 6.10 on page 96 the Web Help for the status that can appear. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: **Connected** - The PPP interface is connected. **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list.
Zone	This field displays the zone to which the interface is assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Services	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network.
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click **Connect** to try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Tunnel Interface Status	This displays the details of the ZyWALL's configured tunnel interfaces.
Name	This field displays the name of the interface.

Table 23 Monitor > System Status > Interface Status (continued)

LABEL	DESCRIPTION
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Zone	This field displays the zone to which the interface is assigned.
IP Address	This is the IP address of the interface. If the interface is active (and connected), the ZyWALL tunnels local traffic sent to this IP address to the **Remote Gateway Address**.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The ZyWALL uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Mode	This field displays the tunnel mode that you are using.
Action	This field lists which services the interface provides to the network. This field displays **n/a** if the interface does not provide any services to the network.
IPv6 Interface Status	This section displays the status of the IPv6 interface. If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is an **Expand** icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.
Port	This field displays the physical port number.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (3G) interfaces, see Section 6.9 on page 93 the Web Help for the status that can appear. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: **Connected** - The PPP interface is connected. **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list.
HA Status	This field displays the status of the interface in the virtual router. **Active** - This interface is the master interface in the virtual router. **Stand-By** - This interface is a backup interface in the virtual router. **Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down. **n/a** - Device HA is not active on the interface.
Zone	This field displays the zone to which the interface is assigned.

Table 23 Monitor > System Status > Interface Status (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IPv6 address assigned to the interface. If the IPv6 address is not displayed, the interface is disabled or did not receive an IPv6 address via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Services	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network.
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click **Connect** to try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Interface Statistics	This table provides packet statistics for each interface.
Refresh	Click this button to update the information in the screen.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface.
Status	This field displays the current status of the interface. **Down** - The interface is not connected. **Speed / Duplex** - The interface is connected. This field displays the port speed and duplex setting (**Full** or **Half**). This field displays **Connected** and the accumulated connection time (hh:mm:ss) when the PPP interface is connected.
TxPkts	This field displays the number of packets transmitted from the ZyWALL on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the ZyWALL on the interface since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.

6.4 The Traffic Statistics Screen

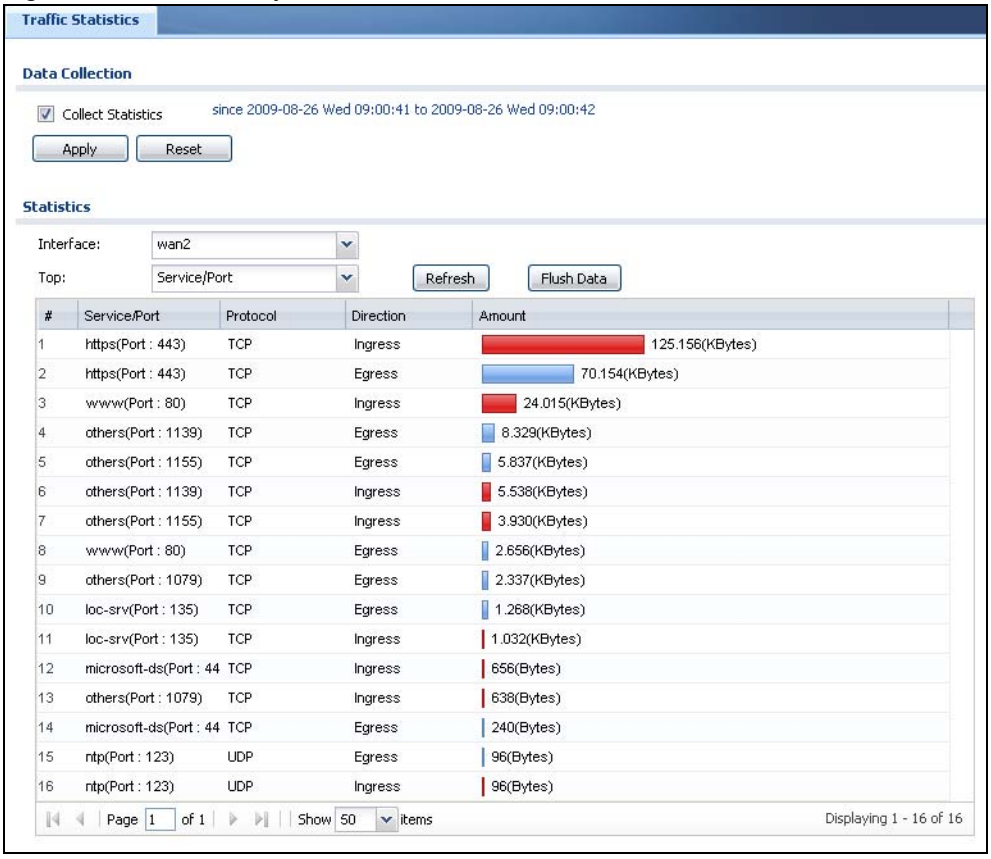
Click **Monitor > System Status > Traffic Statistics** to display the **Traffic Statistics** screen. This screen provides basic information about the following for example:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the ZyWALL counts HTTP GET packets. Please see Table 24 on page 87 for more information.
- Most-used protocols or service ports and the amount of traffic on each one

- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

You use the **Traffic Statistics** screen to tell the ZyWALL when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Traffic Statistics** screen.

Figure 61 Monitor > System Status > Traffic Statistics


Traffic Statistics
Data Collection
Collect Statistics
since 2009-08-26 Wed 09:00:41 to 2009-08-26 Wed 09:00:42
Apply
Reset
Statistics
Interface: wan2
Top: Service/Port
Refresh
Flush Data
Service/Port Protocol Direction Amount
1 https(Port : 443) TCP Ingress 125.156(KBytes)
2 https(Port : 443) TCP Egress 70.154(KBytes)
3 www(Port : 80) TCP Ingress 24.015(KBytes)
4 others(Port : 1139) TCP Egress 8.329(KBytes)
5 others(Port : 1155) TCP Egress 5.837(KBytes)
6 others(Port : 1139) TCP Ingress 5.538(KBytes)
7 others(Port : 1155) TCP Ingress 3.930(KBytes)
8 www(Port : 80) TCP Egress 2.656(KBytes)
9 others(Port : 1079) TCP Egress 2.337(KBytes)
10 loc-srv(Port : 135) TCP Egress 1.268(KBytes)
11 loc-srv(Port : 135) TCP Ingress 1.032(KBytes)
12 microsoft-ds(Port : 44 TCP Ingress 656(Bytes)
13 others(Port : 1079) TCP Ingress 638(Bytes)
14 microsoft-ds(Port : 44 TCP Egress 240(Bytes)
15 ntp(Port : 123) UDP Egress 96(Bytes)
16 ntp(Port : 123) UDP Ingress 96(Bytes)
Page 1 of 1
Show 50 items
Displaying 1 - 16 of 16

There is a limit on the number of records shown in the report. Please see Table 25 on page 89 for more information. The following table describes the labels in this screen.

Table 24 Monitor > System Status > Traffic Statistics

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the ZyWALL collect data for the report. If the ZyWALL has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the **Refresh** button to update it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.
Statistics	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge and PPPoE/PPTP interfaces.

Table 24 Monitor > System Status > Traffic Statistics (continued)

LABEL	DESCRIPTION
Traffic Type	Select the type of report to display. Choices are: **Host IP Address/User** - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. **Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one. **Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited. Each type of report has different information in the report (below).
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
	These fields are available when the **Traffic Type** is **Host IP Address/User**.
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.
IP Address/User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 25 on page 89.
Direction	This field indicates whether the IP address or user is sending or receiving traffic. **Ingress**- traffic is coming from the IP address or user to the ZyWALL. **Egress** - traffic is going from the ZyWALL to the IP address or user.
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 25 on page 89.
	These fields are available when the **Traffic Type** is **Service/Port**.
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the service and port in this record. The maximum number of services and service ports in this report is indicated in Table 25 on page 89.
Protocol	This field indicates what protocol the service was using.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. **Ingress** - traffic is coming into the router through the interface **Egress** - traffic is going out from the router through the interface
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 25 on page 89.
	These fields are available when the **Traffic Type** is **Web Site Hits**.
#	This field is the rank of each record. The domain names are sorted by the number of hits.
Web Site	This field displays the domain names most often visited. The ZyWALL counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 25 on page 89.
Hits	This field displays how many hits the Web site received. The ZyWALL counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the ZyWALL counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 25 on page 89.

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 25 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2^{64} bytes; this is just less than 17 million terabytes.
Hit Count Limit	2^{64} hits; this is over 1.8 x 10^{19} hits.

6.5 The Session Monitor Screen

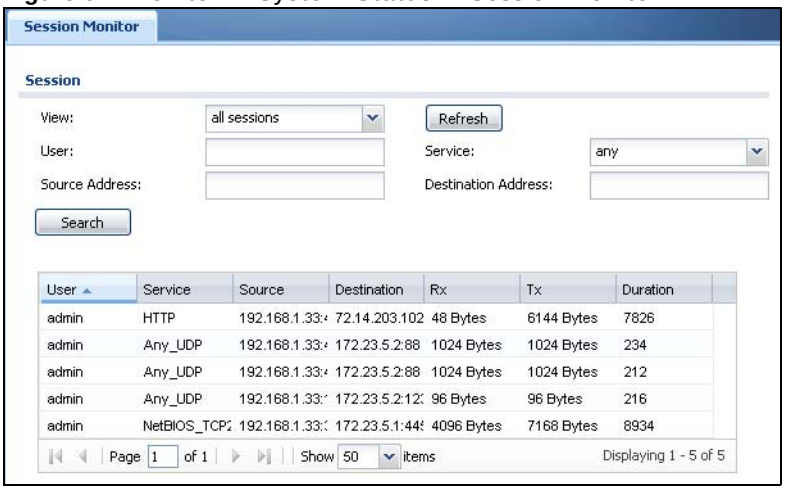
The **Session Monitor** screen displays all established sessions that pass through the ZyWALL for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all established sessions that passed through the ZyWALL by user, service, source IP address, or destination IP address. You can also filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

Click **Monitor > System Status > Session Monitor** to display the following screen.

Figure 62 Monitor > System Status > Session Monitor



The following table describes the labels in this screen.

Table 26 Monitor > System Status > Session Monitor

LABEL	DESCRIPTION
View	Select how you want the established sessions that passed through the ZyWALL to be displayed. Choices are: **sessions by users** - display all active sessions grouped by user **sessions by services** - display all active sessions grouped by service or protocol **sessions by source IP** - display all active sessions grouped by source IP address **sessions by destination IP** - display all active sessions grouped by destination IP address **all sessions** - filter the active sessions by the **User**, **Service**, **Source Address**, and **Destination Address**, and display each session individually (sorted by user).
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The **User**, **Service**, **Source Address**, and **Destination Address** fields display if you view all sessions. Select your desired filter criteria and click the **Search** button to filter the list of sessions.
User	This field displays when **View** is set to **all sessions**. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.
Service	This field displays when **View** is set to **all sessions**. Select the service or service group whose sessions you want to view. The ZyWALL identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 29 on page 390 for more information about services.)
Source	This field displays when **View** is set to **all sessions**. Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination	This field displays when **View** is set to **all sessions**. Type the destination IP address whose sessions you want to view. You cannot include the destination port.
Search	This button displays when **View** is set to **all sessions**. Click this button to update the information on the screen using the filter criteria in the **User**, **Service**, **Source Address**, and **Destination Address** fields.
User	This field displays the user in each active session. If you are looking at the **sessions by users** (or **all sessions**) report, click **+** or **-** to display or hide details about a user's sessions.
Service	This field displays the protocol used in each active session. If you are looking at the **sessions by services** report, click **+** or **-** to display or hide details about a protocol's sessions.
Source	This field displays the source IP address and port in each active session. If you are looking at the **sessions by source IP** report, click **+** or **-** to display or hide details about a source IP address's sessions.
Destination	This field displays the destination IP address and port in each active session. If you are looking at the **sessions by destination IP** report, click **+** or **-** to display or hide details about a destination IP address's sessions.
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

6.6 The DDNS Status Screen

The **DDNS Status** screen shows the status of the ZyWALL's DDNS domain names. Click **Monitor > System Status > DDNS Status** to open the following screen.

Figure 63 Monitor > System Status > DDNS Status


Status
DDNS Status
Update
Profile Name Domain name Effective IP Last Update St Last Update Time
Page 1 of 1 Show 50 items
No data to display

The following table describes the labels in this screen.

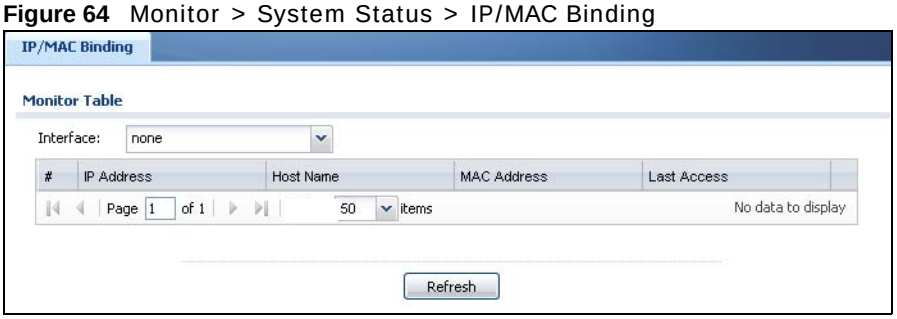
Table 27 Monitor > System Status > DDNS Status

LABEL	DESCRIPTION
Update	Click this to have the ZyWALL update the profile to the DDNS server. The ZyWALL attempts to resolve the IP address for the domain name.
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the ZyWALL can route.
Effective IP	This is the (resolved) IP address of the domain name.
Last Update Status	This shows whether the last attempt to resolve the IP address for the domain name was successful or not. **Updating** means the ZyWALL is currently attempting to resolve the IP address for the domain name.
Last Update Time	This shows when the last attempt to resolve the IP address for the domain name occurred (in year-month-day hour:minute:second format).

6.7 IP/MAC Binding Monitor

Click **Monitor > System Status > IP/MAC Binding** to open the **IP/MAC Binding Monitor** screen. This screen lists the devices that have received an IP address from ZyWALL interfaces with IP/MAC binding enabled and have ever established a session with the ZyWALL. Devices that have never established a session with the ZyWALL do not display in the list.

Figure 64 Monitor > System Status > IP/MAC Binding



The following table describes the labels in this screen.

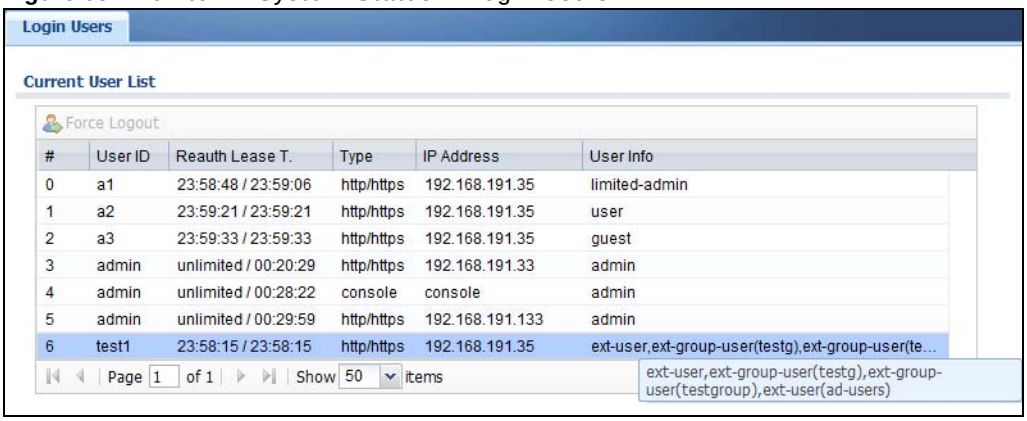
Table 28 Monitor > System Status > IP/MAC Binding

LABEL	DESCRIPTION
Interface	Select a ZyWALL interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address.
#	This is the index number of an IP/MAC binding entry.
IP Address	This is the IP address that the ZyWALL assigned to a device.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests.
MAC Address	This field displays the MAC address to which the IP address is currently assigned.
Last Access	This is when the device last established a session with the ZyWALL through this interface.
Refresh	Click this button to update the information in the screen.

6.8 The Login Users Screen

Use this screen to look at a list of the users currently logged into the ZyWALL. To access this screen, click **Monitor > System Status > Login Users**.

Figure 65 Monitor > System Status > Login Users


Login Users
Current User List
Force Logout
User ID Reauth Lease T. Type IP Address User Info
0 a1 23:58:48 / 23:59:06 http/https 192.168.191.35 limited-admin
1 a2 23:59:21 / 23:59:21 http/https 192.168.191.35 user
2 a3 23:59:33 / 23:59:33 http/https 192.168.191.35 guest
3 admin unlimited / 00:20:29 http/https 192.168.191.33 admin
4 admin unlimited / 00:28:22 console console admin
5 admin unlimited / 00:29:59 http/https 192.168.191.133 admin
6 test1 23:58:15 / 23:58:15 http/https 192.168.191.35 ext-user,ext-group-user(testg),ext-group-user(te...
Page 1 of 1 Show 50 items
ext-user,ext-group-user(testg),ext-group-user(testgroup),ext-user(ad-users)

The following table describes the labels in this screen.

Table 29 Monitor > System Status > Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ZyWALL.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 27 on page 371.
Type	This field displays the way the user logged in to the ZyWALL.
IP Address	This field displays the IP address of the computer used to log in to the ZyWALL.

Table 29 Monitor > System Status > Login Users (continued)

LABEL	DESCRIPTION
User Info	This field displays the types of user accounts the ZyWALL uses. If the user type is **ext-user** (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Force Logout	Select a user ID and click this icon to end a user's session.
Refresh	Click this button to update the information in the screen.

6.9 Cellular Status Screen

This screen displays your 3G connection status. Click **Monitor > System Status > Cellular Status** to display this screen.

Figure 66 Monitor > System Status > Cellular Status


Cellular Status
Cellular Device Status
Refresh
More Information
Extension Slot Connected Device Status Service Provider Cellular System Signal Quality
1 USB 1 Huawei E220 Device ready Chunghwa Telecom WCDMA Excellent
Page 1 of 1 Show 50 items
Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 30 Monitor > System Status > Cellular Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information in the screen.
More Information	Click this to display more information on your 3G, such as the signal strength, IMEA/ESN and IMSI. This is only available when the 3G device attached and activated on your ZyWALL. Refer to Section 6.9.1 on page 95.
#	This field is a sequential value, and it is not associated with any interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the model name of the cellular card.

Table 30 Monitor > System Status > Cellular Status (continued)

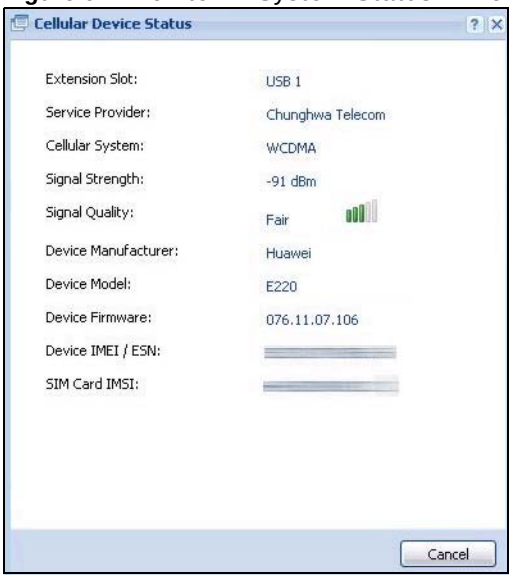
LABEL	DESCRIPTION
Status	**No device** - no 3G device is connected to the ZyWALL. **No Service** - no 3G network is available in the area; you cannot connect to the Internet. **Limited Service** - returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet. **Device detected** - displays when you connect a 3G device. **Device error** - a 3G device is connected but there is an error. **Probe device fail** - the ZyWALL's test of the 3G device failed. **Probe device ok** - the ZyWALL's test of the 3G device succeeded. **Init device fail** - the ZyWALL was not able to initialize the 3G device. **Init device ok** - the ZyWALL initialized the 3G card. **Check lock fail** - the ZyWALL's check of whether or not the 3G device is locked failed. **Device locked** - the 3G device is locked. **SIM error** - there is a SIM card error on the 3G device. **SIM locked-PUK** - the PUK is locked on the 3G device's SIM card. **SIM locked-PIN** - the PIN is locked on the 3G device's SIM card. **Unlock PUK fail** - Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK. **Unlock PIN fail** - Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN. **Unlock device fail** - Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code. **Device unlocked** - You entered the correct device code and unlocked a CDMA2000 3G device. **Get dev-info fail** - The ZyWALL cannot get cellular device information. **Get dev-info ok** - The ZyWALL succeeded in retrieving 3G device information. **Searching network** - The 3G device is searching for a network. **Get signal fail** - The 3G device cannot get a signal from a network. **Network found** - The 3G device found a network. **Apply config** - The ZyWALL is applying your configuration to the 3G device. **Inactive** - The 3G interface is disabled. **Active** - The 3G interface is enabled. **Incorrect device** - The connected 3G device is not compatible with the ZyWALL. **Correct device** - The ZyWALL detected a compatible 3G device. **Set band fail** - Applying your band selection was not successful. **Set band ok** - The ZyWALL successfully applied your band selection. **Set profile fail** - Applying your ISP settings was not successful. **Set profile ok** - The ZyWALL successfully applied your ISP settings. **PPP fail** - The ZyWALL failed to create a PPP connection for the cellular interface. **Need auth-password** - You need to enter the password for the 3G card in the cellular edit screen. **Device ready** - The ZyWALL successfully applied all of your configuration and you can use the 3G connection.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the 3G SIM card. For example if the bill has not been paid or the account has expired.
Cellular System	This field displays what type of cellular network the 3G connection is using. The network type varies depending on the 3G card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM 3G card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA 3G card.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ZyWALL and the service provider's base station.

6.9.1 More Information

This screen displays more information on your 3G, such as the signal strength, IMEA/ESN and IMSI that helps identify your 3G device and SIM card. Click **Monitor > System Status > More Information** to display this screen.

Note: This screen is only available when the 3G device is attached to and activated on the ZyWALL.

Figure 67 Monitor > System Status > More Information



The following table describes the labels in this screen.

Table 31 Monitor > System Status > More Information

LABEL	DESCRIPTION
Extension Slot	This field displays where the entry's cellular card is located.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the 3G SIM card. For example if the bill has not been paid or the account has expired.
Cellular System	This field displays what type of cellular network the 3G connection is using. The network type varies depending on the 3G card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM 3G card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA 3G card.
Signal Strength	This is the **Signal Quality** measured in dBm.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ZyWALL and the service provider's base station.
Device Manufacturer	This shows the name of the company that produced the 3G device.
Device Model	This field displays the model name of the cellular card.
Device Firmware	This shows the software version of the 3G device.

Table 31 Monitor > System Status > More Information (continued)

LABEL	DESCRIPTION
Device IMEI/ESN	IMEI (International Mobile Equipment Identity) is a 15-digit code in decimal format that identifies the 3G device. ESN (Electronic Serial Number) is an 8-digit code in hexadecimal format that identifies the 3G device.
SIM Card IMSI	IMSI (International Mobile Subscriber Identity) is a 15-digit code that identifies the SIM card.

6.10 USB Storage Screen

This screen displays information about a connected USB storage device. Click **Monitor > System Status > USB Storage** to display this screen.

Figure 68 Monitor > System Status > USB Storage



The following table describes the labels in this screen.

Table 32 Monitor > System Status > USB Storage

LABEL	DESCRIPTION
Device description	This is a basic description of the type of USB device.
Usage	This field displays how much of the USB storage device's capacity is currently being used out of its total capacity and what percentage that makes.
Filesystem	This field displays what file system the USB storage device is formatted with. This field displays **Unknown** if the file system of the USB storage device is not supported by the ZyWALL, such as NTFS.
Speed	This field displays the connection speed the USB storage device supports.

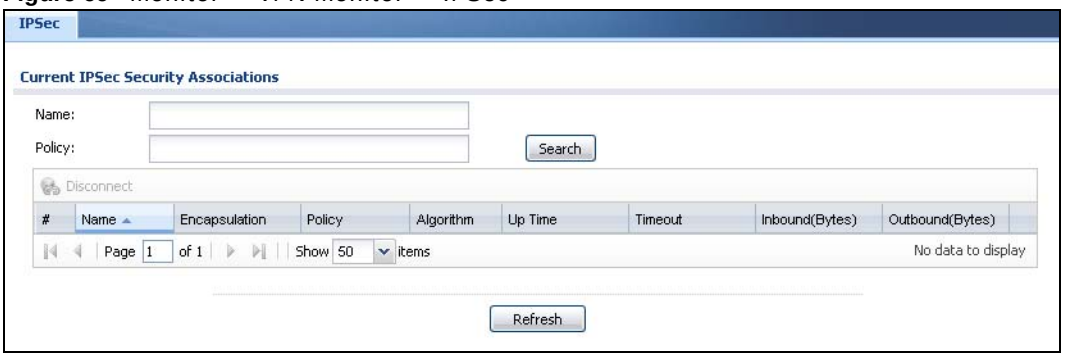
Table 32 Monitor > System Status > USB Storage (continued)

LABEL	DESCRIPTION
Status	**Ready** - you can have the ZyWALL use the USB storage device. Click **Remove Now** to stop the ZyWALL from using the USB storage device so you can remove it. **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the ZyWALL cannot mount it. Click **Use It** to have the ZyWALL mount a connected USB storage device. This button is grayed out if the file system is not supported (unknown) by the ZyWALL. **none** - no USB storage device is connected.
Detail	This field displays any other information the ZyWALL retrieves from the USB storage device. **Deactivated** - the use of a USB storage device is disabled (turned off) on the ZyWALL. **OutofSpace** - the available disk space is less than the disk space full threshold (see Section 37.2 on page 444 for how to configure this threshold). **Mounting** - the ZyWALL is mounting the USB storage device. **Removing** - the ZyWALL is unmounting the USB storage device. **none** - the USB device is operating normally or not connected.

6.11 The IPSec Monitor Screen

You can use the **IPSec Monitor** screen to display and to manage active IPSec To access this screen, click **Monitor > VPN Monitor** > **IPSec**. The following screen appears. SAs. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 69 Monitor > VPN Monitor > IPSec



Each field is described in the following table.

Table 33 Monitor > VPN Monitor > IPSec

LABEL	DESCRIPTION
Name	Enter the name of a IPSec SA here and click **Search** to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 6.11.1 on page 98 for more details.
Policy	Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 6.11.1 on page 98 for more details.
Search	Click this button to search for an IPSec SA that matches the information you specified above.
Disconnect	Select an IPSec SA and click this button to disconnect it.
Total Connection	This field displays the total number of associated IPSec SAs.
connection per page	Select how many entries you want to display on each page.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Policy	This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Up Time	This field displays how many seconds the IPSec SA has been active. This field displays **N/A** if the IPSec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the ZyWALL automatically disconnects the IPSec SA. This field displays **N/A** if the IPSec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the ZyWALL since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the ZyWALL to the remote IPSec router since the IPSec SA was established.
Refresh	Click **Refresh** to update the information in the display.

6.11.1 Regular Expressions in Searching IPSec SAs

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use “*abc” (without the quotation marks) to specify any VPN connection or policy name that ends with “abc”. A VPN connection named “testabc” would match. There could be any number (of any type) of characters in front of the “abc” at the end and the VPN connection or policy name would still match. A VPN connection or policy name named “testacc” for example would not match.

A * in the middle of a VPN connection or policy name has the ZyWALL check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

6.12 The SSL Connection Monitor Screen

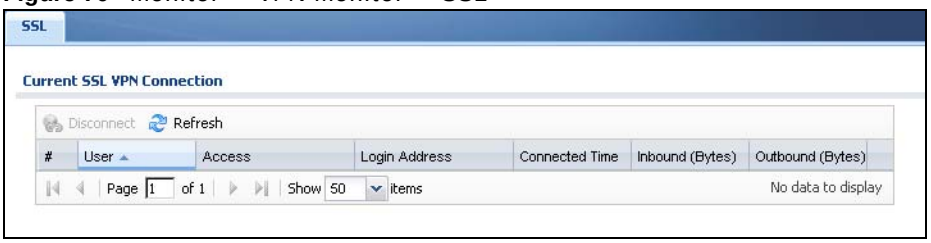
The ZyWALL keeps track of the users who are currently logged into the VPN SSL client Click **Monitor > VPN Monitor > SSL** to display the user list.

portal. Use this screen to do the following:

- View a list of active SSL VPN connections.
- Log out individual users and delete related session information.

Once a user logs out, the corresponding entry is removed from the **Connection Monitor** screen.

Figure 70 Monitor > VPN Monitor > SSL



The following table describes the labels in this screen.

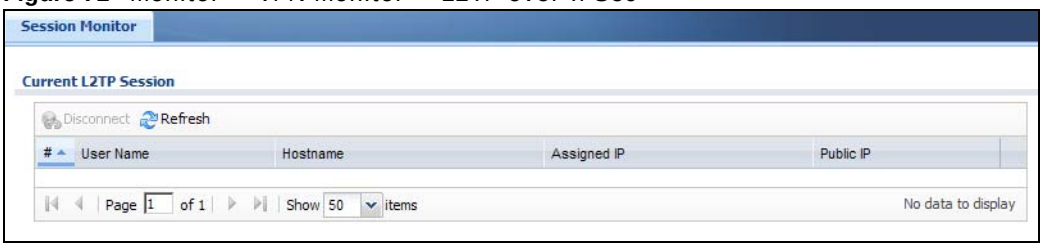
Table 34 Monitor > VPN Monitor > SSL

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to terminate the user's connection and delete corresponding session information from the ZyWALL.
#	This field displays the index number.
User	This field displays the account user name used to establish this SSL VPN connection.
Access	This field displays the name of the SSL VPN application the user is accessing.
Login Address	This field displays the IP address the user used to establish this SSL VPN connection.
Connected Time	This field displays the time this connection was established.
Inbound (Bytes)	This field displays the number of bytes received by the ZyWALL on this connection.
Outbound (Bytes)	This field displays the number of bytes transmitted by the ZyWALL on this connection.
Refresh	Click **Refresh** to update this screen.

6.13 The L2TP over IPSec Session Monitor Screen

Click **Monitor > VPN Monitor > L2TP over IPSec** to open the following screen. Use this screen to display and manage the ZyWALL's connected L2TP VPN sessions.

Figure 71 Monitor > VPN Monitor > L2TP over IPSec



The following table describes the fields in this screen.

Table 35 Monitor > VPN Monitor > L2TP over IPSec

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to disconnect it.
#	This is the index number of a current L2TP VPN session.
User Name	This field displays the remote user's user name.
Hostname	This field displays the name of the computer that has this L2TP VPN connection with the ZyWALL.
Assigned IP	This field displays the IP address that the ZyWALL assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This field displays the public IP address that the remote user is using to connect to the Internet.
Refresh	Click **Refresh** to update this screen.

6.14 Log Screen

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, firewall or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

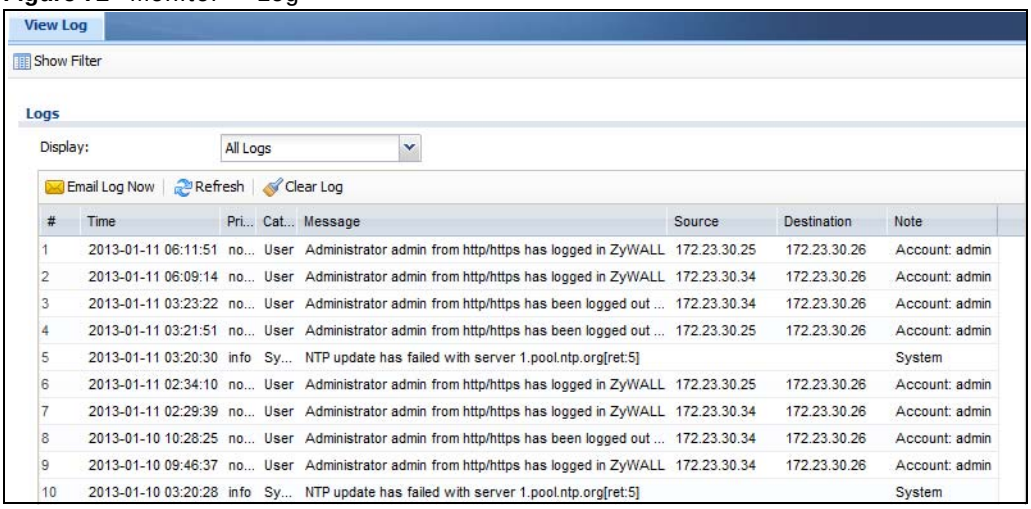
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

- The maximum possible number of log messages in the ZyWALL varies by model.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 72 Monitor > Log


View Log
Show Filter
Logs
Display:
All Logs
Email Log Now
Refresh
Clear Log
Time Pri... Cat... Message Source Destination Note
1 2013-01-11 06:11:51 no... User Administrator admin from http/https has logged in ZyWALL 172.23.30.25 172.23.30.26 Account: admin
2 2013-01-11 06:09:14 no... User Administrator admin from http/https has logged in ZyWALL 172.23.30.34 172.23.30.26 Account: admin
3 2013-01-11 03:23:22 no... User Administrator admin from http/https has been logged out ... 172.23.30.34 172.23.30.26 Account: admin
4 2013-01-11 03:21:51 no... User Administrator admin from http/https has been logged out ... 172.23.30.25 172.23.30.26 Account: admin
5 2013-01-11 03:20:30 info Sy... NTP update has failed with server 1.pool.ntp.org[ret:5] System
6 2013-01-11 02:34:10 no... User Administrator admin from http/https has logged in ZyWALL 172.23.30.25 172.23.30.26 Account: admin
7 2013-01-11 02:29:39 no... User Administrator admin from http/https has logged in ZyWALL 172.23.30.34 172.23.30.26 Account: admin
8 2013-01-10 10:28:25 no... User Administrator admin from http/https has been logged out ... 172.23.30.34 172.23.30.26 Account: admin
9 2013-01-10 09:46:37 no... User Administrator admin from http/https has logged in ZyWALL 172.23.30.34 172.23.30.26 Account: admin
10 2013-01-10 03:20:28 info Sy... NTP update has failed with server 1.pool.ntp.org[ret:5] System

The following table describes the labels in this screen.

Table 36 Monitor > Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Service**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Service	This displays when you show the filter. Select the service whose log messages you would like to see. The Web Configurator uses the protocol and destination port number(s) of the service to select which log messages you see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.

Table 36 Monitor > Log (continued)

LABEL	DESCRIPTION
Email Log Now	Click this button to send log message(s) to the **Active** e-mail address(es) specified in the **Send Log To** field on the **Log Settings** page (see Section 38.3.2 on page 489).
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on (see **Log Consolidation** in Table 196 on page 490). and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

7

Interfaces

7.1 Interface Overview

Use the **Interface** screens to configure the ZyWALL's interfaces. You can also create interfaces on top of other interfaces.

- **Ports** are the physical ports to which you connect cables.
- **Interfaces** are used within the system operationally. You use them in configuring various features. An interface also describes a network that is directly connected to the ZyWALL. For example, You connect the LAN network to the LAN interface.
- **Zones** are groups of interfaces used to ease security policy configuration.

7.1.1 What You Can Do in this Chapter

- Use the **Port Role** screen (Section 7.2 on page 108) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Ethernet** screens (Section 7.3 on page 109) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Use the **PPP** screens (Section 7.4 on page 125) for PPPoE or PPTP Internet connections.
- Use the **Cellular** screens (Section 7.5 on page 132) to configure settings for interfaces for Internet connections through an installed 3G card.
- Use the **Tunnel** screens (Section 7.6 on page 140) to configure tunnel interfaces to be used in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.
- Use the **VLAN** screens (Section 7.7 on page 147) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the **Bridge** screens (Section 7.8 on page 159) to combine two or more network segments into a single network.
- Use the **Virtual Interface** screen (Section 7.9.1 on page 171) to create virtual interfaces on top of Ethernet interfaces to tell the ZyWALL where to route packets. You can create virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Use the **Trunk** screens (Chapter 8 on page 177) to configure load balancing.

7.1.2 What You Need to Know

Interface Characteristics

Interfaces generally have the following characteristics (although not all characteristics apply to each type of interface).

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface belongs to at most one zone.
- Many interfaces can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Types of Interfaces

You can create several types of interfaces in the ZyWALL.

- Setting interfaces to the same port role forms a port group. Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. Port groups are created when you use the **Interface > Port Roles** screen to set multiple physical ports to be part of the same interface.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **Tunnel interfaces** send IPv4 or IPv6 packets from one network to a specific network through the Internet or a public network.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL. You can also assign an IP address and subnet mask to the bridge.
- **PPP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **Virtual interfaces** provide additional routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **Trunk interfaces** manage load balancing between interfaces.

Port groups and trunks have a lot of characteristics that are specific to each type of interface. The other types of interfaces--Ethernet, PPP, cellular, VLAN, bridge, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 37 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Name*	wan1	lan1, lan2, dmz	ppp*x*	cellular*x*	vlan*x*	br*x*	**
Configurable Zone	No	No	Yes	Yes	Yes	Yes	No
IP Address Assignment							
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters							
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 37 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics (continued)

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No
DHCP							
DHCP server	No	Yes	No	No	Yes	Yes	No
DHCP relay	No	Yes	No	No	Yes	Yes	No
Connectivity Check	Yes	No	Yes	Yes	Yes	Yes	No

- * The format of interface names other than the Ethernet and ppp interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, lan1, lan2, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

Relationships Between Interfaces

In the ZyWALL, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports or port groups. The relationships between interfaces are explained in the following table.

Table 38 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPP interface	Ethernet interface* VLAN interface* bridge interface WAN1, WAN2, OPT*
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPP interface

* - You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

IPv6 Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) from the left is the network prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 39 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the ZyWALL's WAN interface is connected to an ISP with a router and the ZyWALL is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

Prefix Delegation

Prefix delegation enables an IPv6 router (the ZyWALL) to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The ZyWALL uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the router passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

IPv6 Router Advertisement

An IPv6 router sends router advertisement messages periodically to advertise its presence and other parameters to the hosts in the same network.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Finding Out More

- See Section 7.10 on page 172 for background information on interfaces.
- See Chapter 8 on page 177 to configure load balancing using trunks.

1. In IPv6, all network interfaces can be associated with several addresses.

7.1.3 What You Need to Do First

For IPv6 settings, go to the **Configuration** > **System** > **IPv6** screen to enable IPv6 support on the ZyWALL first.

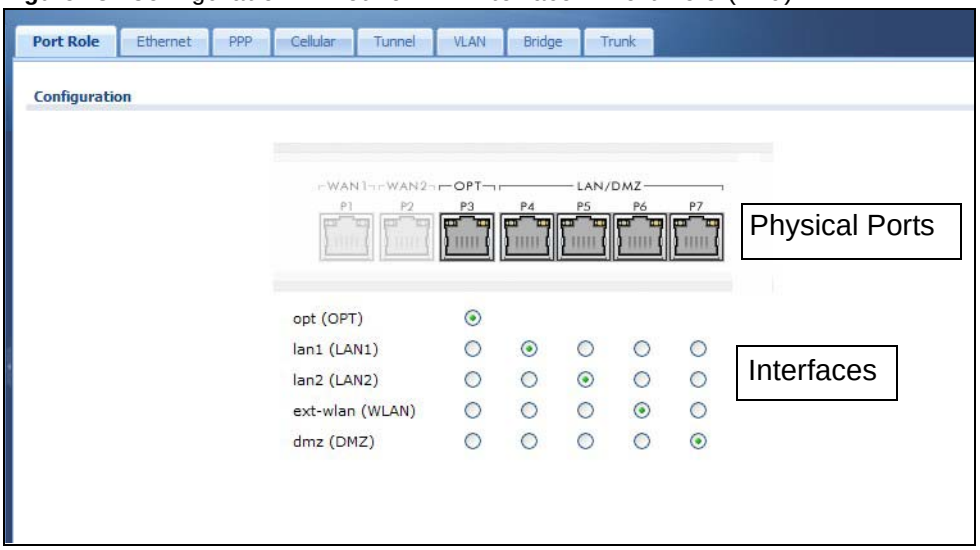
7.2 Port Role Screen

To access this screen, click **Configuration > Network > Interface > Port Role**. Use the **Port Role** screen to set the ZyWALL's flexible ports as part of the **lan1**, **lan2**, **ext-wlan** or **dmz** interfaces. This creates a hardware connection between the physical ports at the layer-2 (data link, MAC address) level. This provides wire-speed throughput but no security.

Not the following if you are configuring from a computer connected to a **lan1**, **lan2**, **ext-wlan** or **dmz** port and change the port's role:

- A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's **lan1**, **lan2**, **ext-wlan** or **dmz** IP address.
- Use the appropriate **lan1**, **lan2**, **ext-wlan** or **dmz** IP address to access the ZyWALL.

Figure 73 Configuration > Network > Interface > Port Role (110)



The physical Ethernet ports are shown at the top and the Ethernet interfaces and zones are shown at the bottom of the screen. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port's LAN radio button to use the port as part of the LAN interface. The port will use the ZyWALL's LAN IP address and MAC address.

When you assign more than one physical port to a network, you create a **port group**. Port groups have the following characteristics:

- There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.
- It can increase the bandwidth between the port group and other interfaces.
- The port group uses a single MAC address.

Click **Apply** to save your changes and apply them to the ZyWALL.

Click **Reset** to change the port groups to their current configuration (last-saved values).

7.3 Ethernet Summary Screen

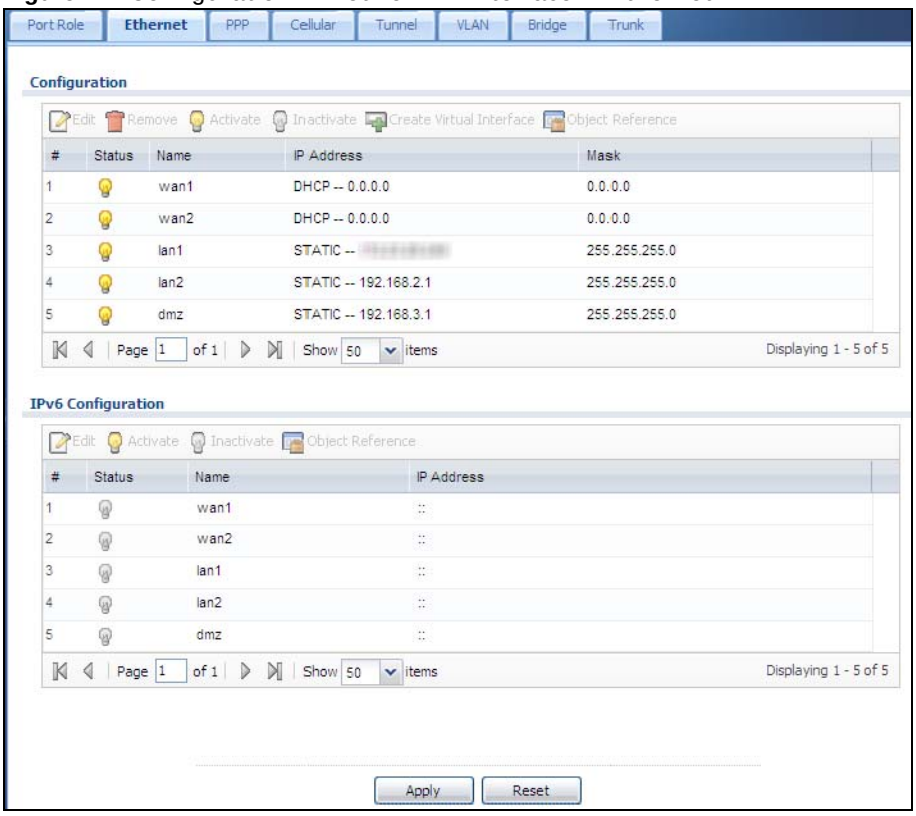
This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure Ethernet interfaces used for your IPv6 networks on this screen. To access this screen, click **Configuration > Network** > **Interface > Ethernet**.

Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it, the Ethernet interface is effectively removed from the ZyWALL, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

Use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management. The ZyWALL supports two routing protocols, RIP and OSPF. See Chapter 10 on page 199 for background information about these routing protocols.

Figure 74 Configuration > Network > Interface > Ethernet



Each field is described in the following table.

Table 40 Configuration > Network > Interface > Ethernet

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your ZyWALL to an IPv6 network. Both sections have similar fields as described below.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a virtual interface, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an interface, select it and click **Activate**.
Inactivate	To turn off an interface, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual Ethernet interface, select an Ethernet interface and click **Create Virtual Interface**.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or :: (in the IPv6 network), the interface does not have an IP address yet. In the IPv4 network, this screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. In the IPv6 network, this screen also shows whether the IP address is a static IP address (**STATIC**), link-local IP address (**LINK LOCAL**), dynamically assigned (**DHCP**), or an IPv6 StateLess Address AutoConfiguration IP address (**SLAAC**). See Section 7.1.2 on page 103 for more information about IPv6.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.3.1 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, connectivity check, and MAC address settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See Section 7.3 on page 109.)

Note: If you create IP address objects based on an interface's IP address, subnet, or gateway, the ZyWALL automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change the LAN's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN subnet address object.

With RIP, you can use Ethernet interfaces to do the following things.

- Enable and disable RIP in the underlying physical port or port group.

- Select which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The ZyWALL supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The ZyWALL can use subnet broadcasting or multicasting.

With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Set the priority used to identify the DR or BDR if one does not exist.

Figure 75 Configuration > Network > Interface > Ethernet > Edit (External Type)

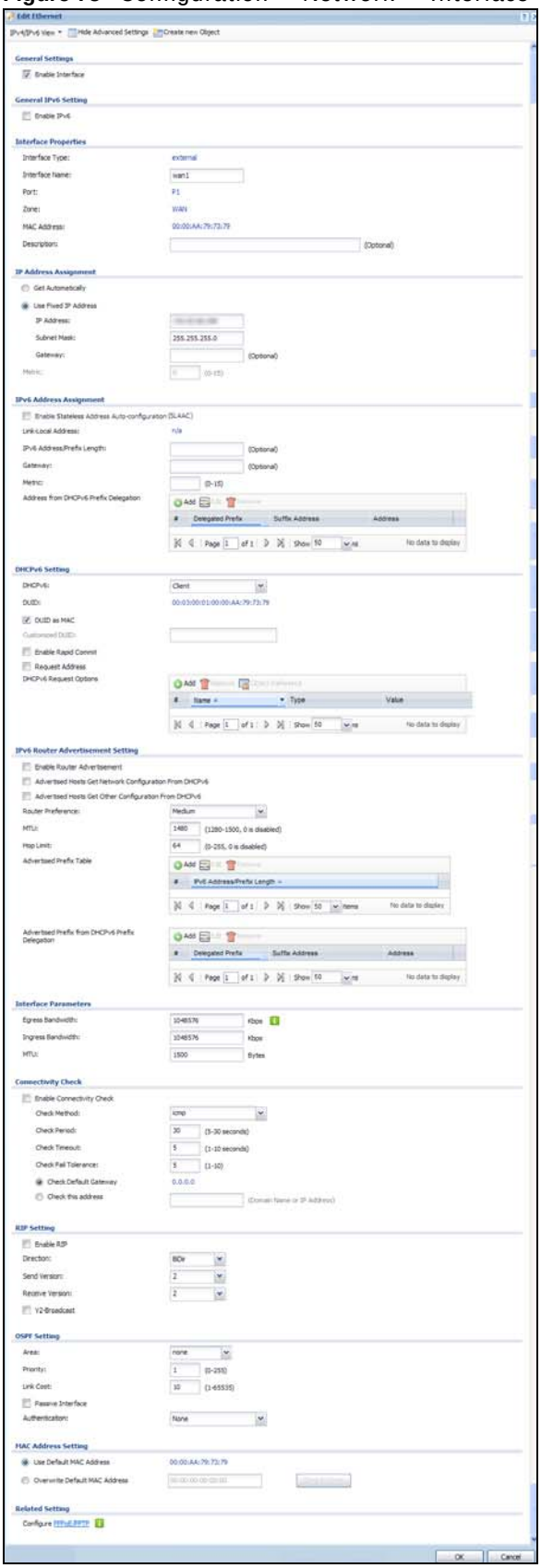


Figure 76 Configuration > Network > Interface > Ethernet > Edit (Internal Type)

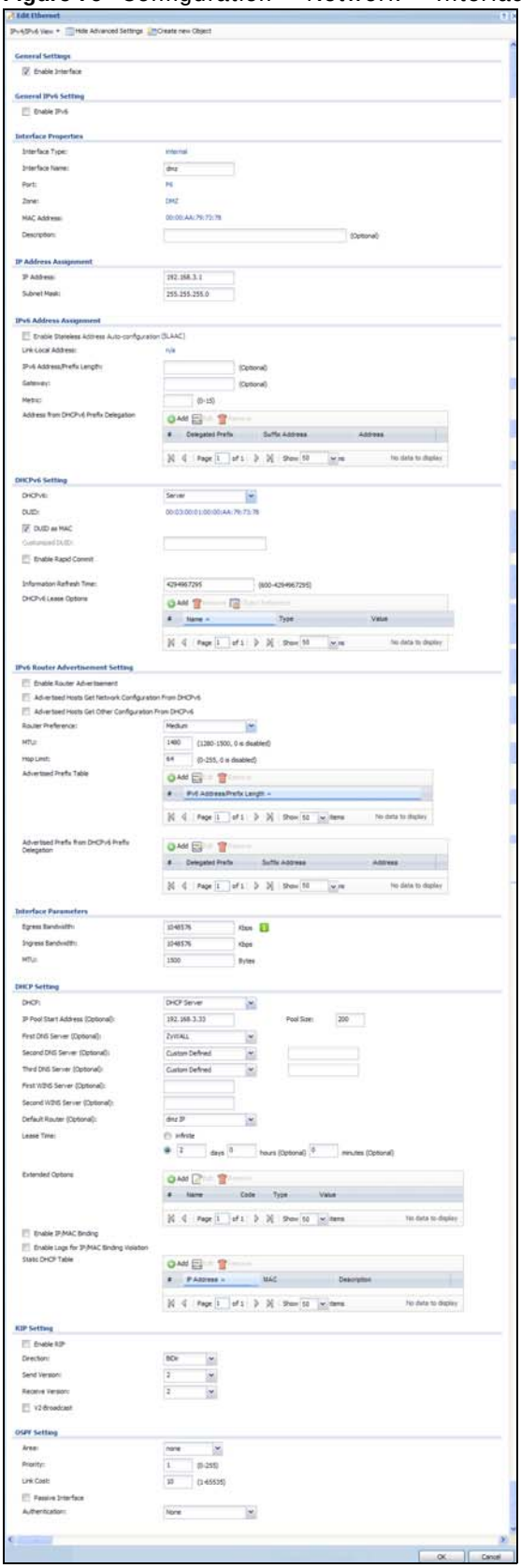
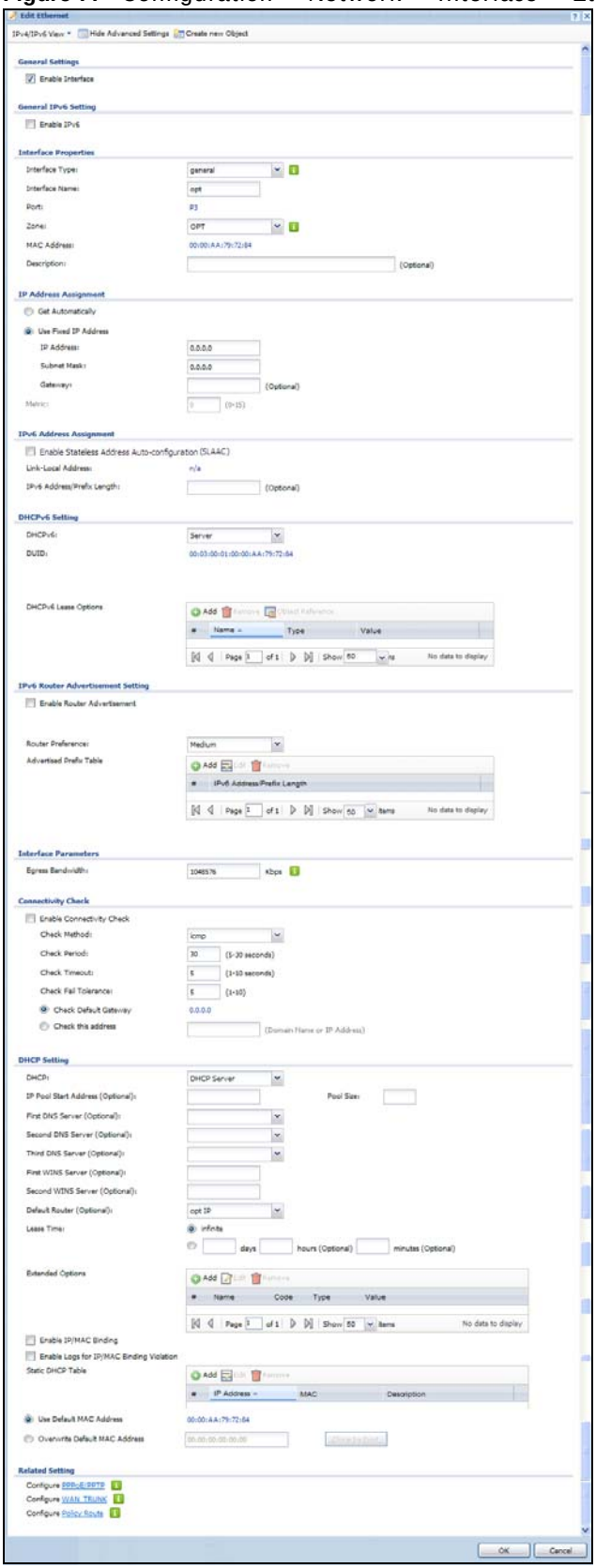


Figure 77 Configuration > Network > Interface > Ethernet > Edit (OPT)



This screen's fields are described in the table below.

Table 41 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	This field is configurable for the **OPT** interface only. Select to which type of network you will connect this interface. When you select **internal** or **external** the rest of the screen's options automatically adjust to correspond. The ZyWALL automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The ZyWALL automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as firewall, remote management.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `( )+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	These IP address fields configure an IPv4 IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when **Interface Type** is **external** or **general**. Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server. You should not select this if the interface is assigned to a VRRP group. See Chapter 26 on page 359.
Use Fixed IP Address	This option appears when **Interface Type** is **external** or **general**. Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This option appears when **Interface Type** is **external** or **general**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when **Interface Type** is **external** or **general**. Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the ZyWALL generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the ZyWALL obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 107 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 107 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what additional information to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 7.3.3 on page 123 for more information.
Remove	Select an entry and click this to delete it from this table.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the ZyWALL obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 107 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the ZyWALL. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL discards the packet and sends an error message to the sender to inform this.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the ZyWALL to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	This table is available when the **Interface Type** is **internal**. Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The ZyWALL will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	These fields appear when **Interface Properties** is **External** or **General**. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
DHCP Setting	This section appears when **Interface Type** is **internal** or **general**.
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire. **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 7.3.4 on page 124.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.
Value	This is the value set for the DHCP option.

Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ZyWALL assigns to computers connected to the interface. Otherwise, the ZyWALL assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.2 on page 199 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting.
OSPF Setting	See Section 10.3 on page 201 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.

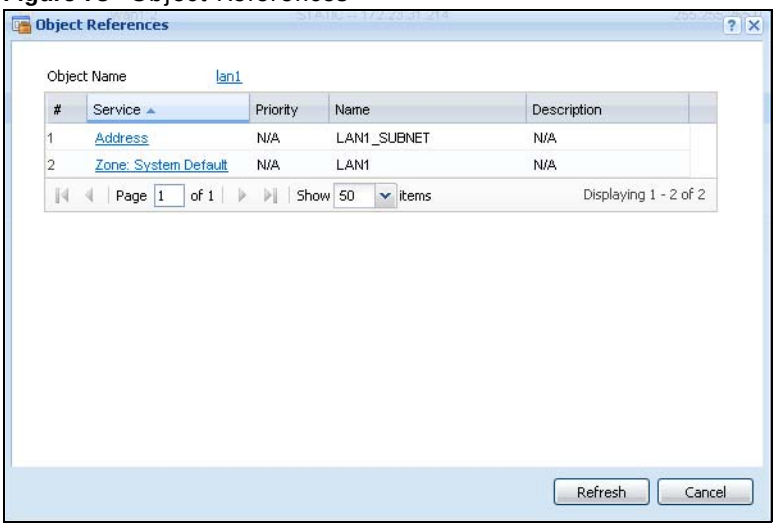
Table 41 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when **Interface Properties** is **External** or **General**. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the ZyWALL uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click **Clone by host** and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Related Setting	
Configure PPPoE/PPTP	Click **PPPoE/PPTP** if this interface's Internet connection uses PPPoE or PPTP.
Configure VLAN	Click **VLAN** if you want to configure a VLAN interface for this Ethernet interface.
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can set this interface to be part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the policy route summary screen where you can manually associate traffic with this interface. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **general**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with an **Interface Type** of **internal** or **external**.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.3.2 Object References

When a configuration screen includes an **Object Reference** icon, select a configuration object and click **Object Reference** to open the **Object References** screen. This screen displays which configuration settings reference the selected object. The fields shown vary with the type of object.

Figure 78 Object References



The following table describes labels that can appear in this screen.

Table 42 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

7.3.3 Add/Edit DHCPv6 Request/Release Options

When you configure an interface as a DHCPv6 server or client, you can additionally add DHCPv6 request or lease options which have the ZyWALL to add more information in the DHCPv6 packets. To open the screen, click **Configuration > Network > Interface > Ethernet > Edit**, select **DHCPv6 Server** or **DHCPv6 Client** in the **DHCPv6 Setting** section, and then click **Add** in the **DHCPv6 Request Options** or **DHCPv6 Lease Options** table.

Figure 79 Configuration > Network > Interface > Ethernet > Edit > Add DHCPv6 Request/Lease Options

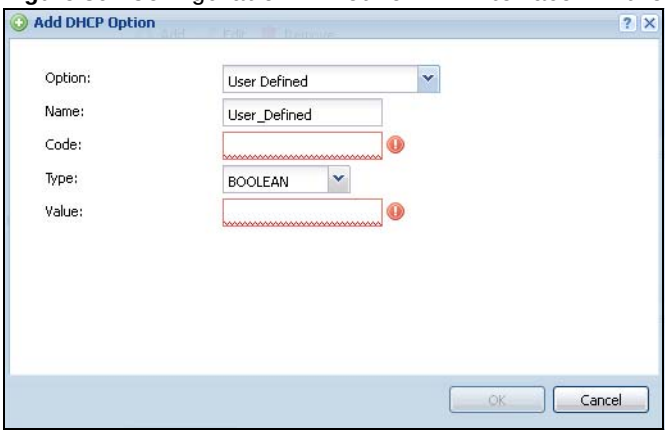


Select a DHCPv6 request or lease object in the **Select one object** field and click **OK** to save it. Click **Cancel** to exit without saving the setting.

7.3.4 Add/Edit DHCP Extended Options

When you configure an interface as a DHCPv4 server, you can additionally add DHCP extended options which have the ZyWALL to add more information in the DHCP packets. The available fields vary depending on the DHCP option you select in this screen. To open the screen, click **Configuration > Network > Interface > Ethernet > Edit**, select **DHCP Server** in the **DHCP Setting** section, and then click **Add** or **Edit** in the **Extended Options** table.

Figure 80 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options



The following table describes labels that can appear in this screen.

Table 43 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface. See Table 44 for more information.
Name	This field displays the name of the selected DHCP option. If you selected **User Defined** in the **Option** field, enter a descriptive name to identify the DHCP option. You can enter up to 16 characters (“a-z”, “A-Z, “0-9”, “-”, and “_”) with no spaces allowed. The first character must be alphabetical (a-z, A-Z).
Code	This field displays the code number of the selected DHCP option. If you selected **User Defined** in the **Option** field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected **User Defined** in the **Option** field, select an appropriate type for the value that you will enter in the next field. Only advanced users should configure **User Defined**. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected **TFTP Server Name (66)** and the type is **TEXT**, enter the DNS domain name of a TFTP server here. This field is mandatory.
First IP Address, Second IP Address, Third IP Address	If you selected **Time Server (4)**, **NTP Server (41)**, **SIP Server (120)**, **CAPWAP AC (138)**, or **TFTP Server (150)**, you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First Enterprise ID, Second Enterprise ID	If you selected **VIVC (124)** or **VIVS (125)**, you have to enter at least one vendor’s 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.
First Class, Second Class	If you selected **VIVC (124)**, enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.

Table 43 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
First Information, Second Information	If you selected **VIVS (125)**, enter additional information for the corresponding enterprise number in these fields.
OK	Click this to close this screen and update the settings to the previous Edit screen.
Cancel	Click **Cancel** to close the screen.

The following table lists the available DHCP extended options (defined in RFCs) on the ZyWALL. See RFCs for more information.

Table 44 DHCP Extended Options

OPTION NAME	CODE	DESCRIPTION
Time Offset	2	This option specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Time Server	4	This option specifies a list of Time servers available to the client.
NTP Server	42	This option specifies a list of the NTP servers available to the client by IP address.
TFTP Server Name	66	This option is used to identify a TFTP server when the “sname” field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
Bootfile	67	This option is used to identify a bootfile when the “file” field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
SIP Server	120	This option carries either an IPv4 address or a DNS domain name to be used by the SIP client to locate a SIP server.
VIVC	124	Vendor-Identifying Vendor Class option A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.
VIVS	125	Vendor-Identifying Vendor-Specific option DHCP clients and servers may use this option to exchange vendor-specific information.
CAPWAP AC	138	CAPWAP Access Controller addresses option The Control And Provisioning of Wireless Access Points Protocol allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers to which it is to connect. This option carries a list of IPv4 addresses indicating one or more CAPWAP ACs available to the WTP.
TFTP Server	150	The option contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

7.4 PPP Interfaces

Use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

Figure 81 Example: PPPoE/PPTP Interfaces



PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

- You must also configure an ISP account object for the PPPoE/PPTP interface to use.

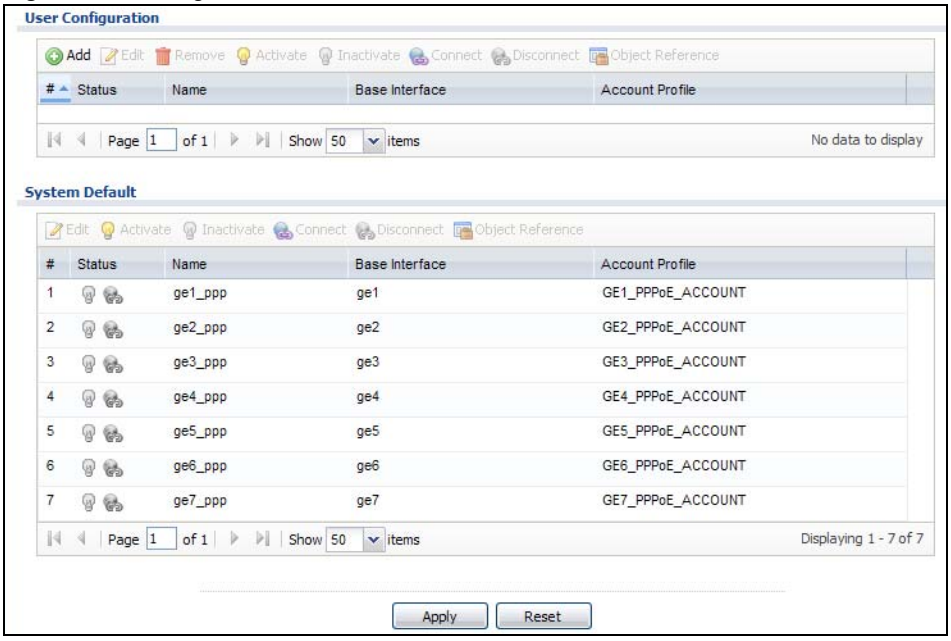
  Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.
- You do not set up the subnet mask or gateway.

  PPPoE/PPTP interfaces are interfaces between the ZyWALL and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the ZyWALL always treats the ISP as a gateway.

7.4.1 PPP Interface Summary

This screen lists every PPPoE/PPTP interface. To access this screen, click **Configuration > Network** > **Interface** > **PPP**.

Figure 82 Configuration > Network > Interface > PPP



Each field is described in the table below.

Table 45 Configuration > Network > Interface > PPP

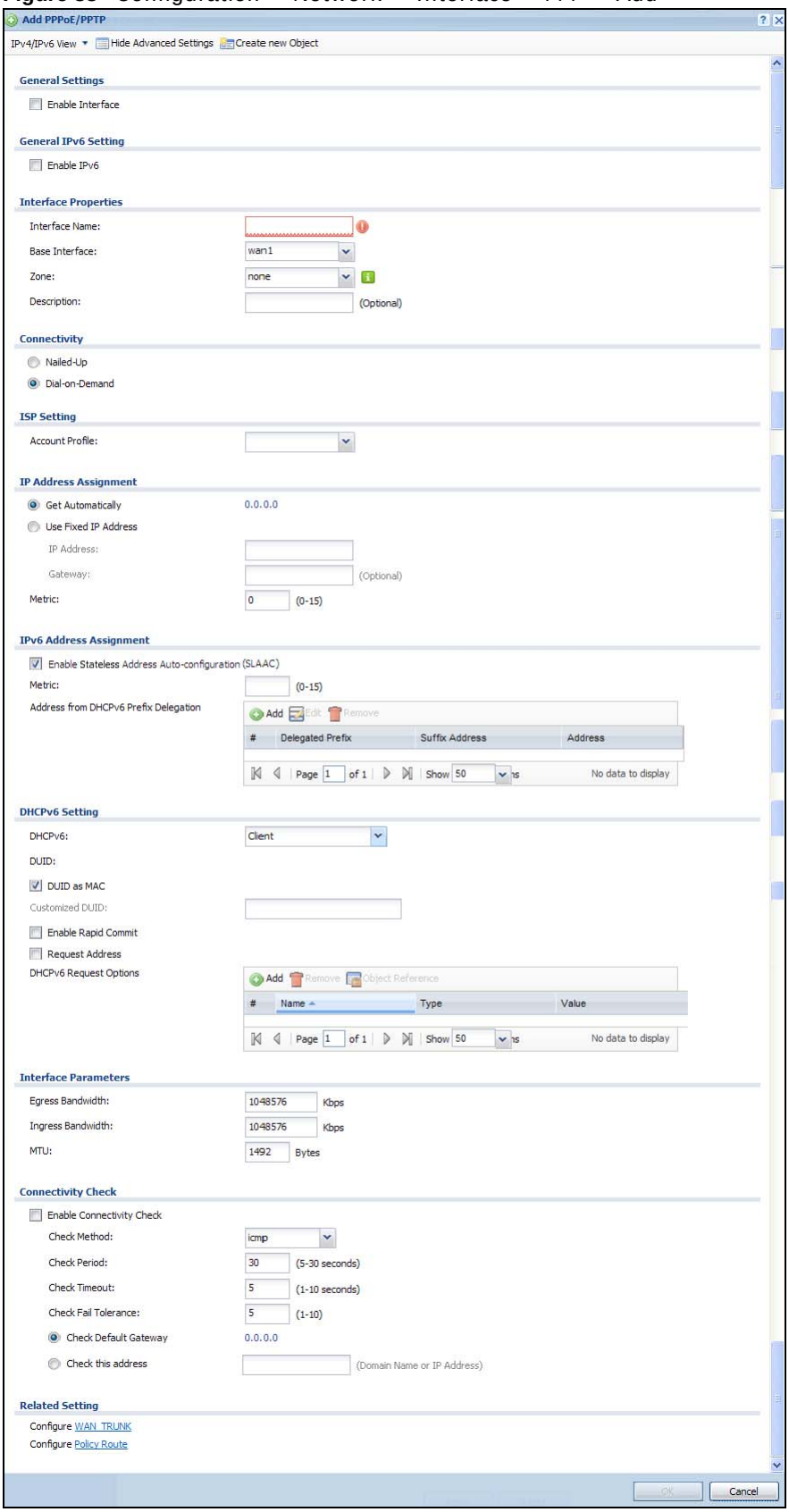
LABEL	DESCRIPTION
User Configuration / System Default	The ZyWALL comes with the (non-removable) **System Default** PPP interfaces pre-configured. You can create (and delete) **User Configuration** PPP interfaces.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.4.2 PPP Interface Add or Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure a PPPoE or PPTP interface. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure PPP interfaces used for your IPv6 networks on this screen. To access this screen, click the **Add** icon or an **Edit** icon in the PPP Interface screen.

Figure 83 Configuration > Network > Interface > PPP > Add



Each field is explained in the following table.

Table 46 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create an ISP Account or a DHCPv6 request object that you may use for the ISP or DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which this PPP interface belongs. The zone determines the security settings the ZyWALL uses for the interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP connection should always be up. Clear this to have the ZyWALL establish the PPPoE/PPTP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the ZyWALL establish the PPPoE/PPTP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name. Use **Create new Object** if you need to configure a new ISP account (see Chapter 34 on page 429 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	Click **Show Advanced Settings** to display more settings. Click **Hide Advanced Settings** to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.

Table 46 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the ZyWALL obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 107 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select **Client** to obtain an IP address and DNS information from the service provider for the interface. Otherwise, select **N/A** to diable the function.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 107 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.

Table 46 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Request Address	Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options	Use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.
Add	Click this to create an entry in this table. See Section 7.3.4 on page 124 for more information.
Remove	Select an entry and click this to delete it from this table.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the ZyWALL will advertise to its clients.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.

Table 46 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.5 Cellular Configuration Screen (3G)

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the 3G device you use, the signal strength to the service provider's base station, and so on.

You can configure how the ZyWALL's 3G device connects to a network (refer to Section 7.5.1 on page 134):

- You can set the 3G device to connect only to the home network, which is the network to which you are originally subscribed.
- You can set the 3G device to connect to other networks if the signal strength of the home network is too low or it is unavailable.

Aside from selecting the 3G network, the 3G card may also select an available 2.5G or 2.75G network automatically. See the following table for a comparison between 2G, 2.5G, 2.75G and 3G of wireless technologies.

Table 47 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.	CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		Fast

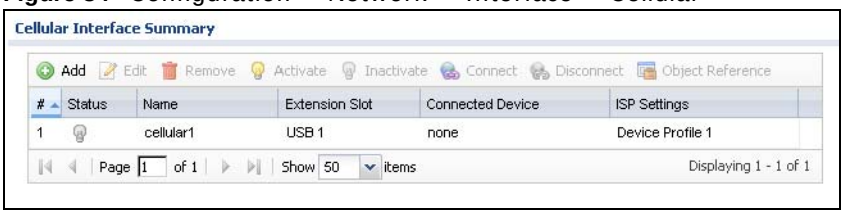
A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

To change your 3G WAN settings, click **Configuration > Network > Interface** > **Cellular**.

Note: Install (or connect) a compatible 3G USB device to use a cellular connection.

Note: The WAN IP addresses of a ZyWALL with multiple WAN interfaces must be on different subnets.

Figure 84 Configuration > Network > Interface > Cellular



The following table describes the labels in this screen.

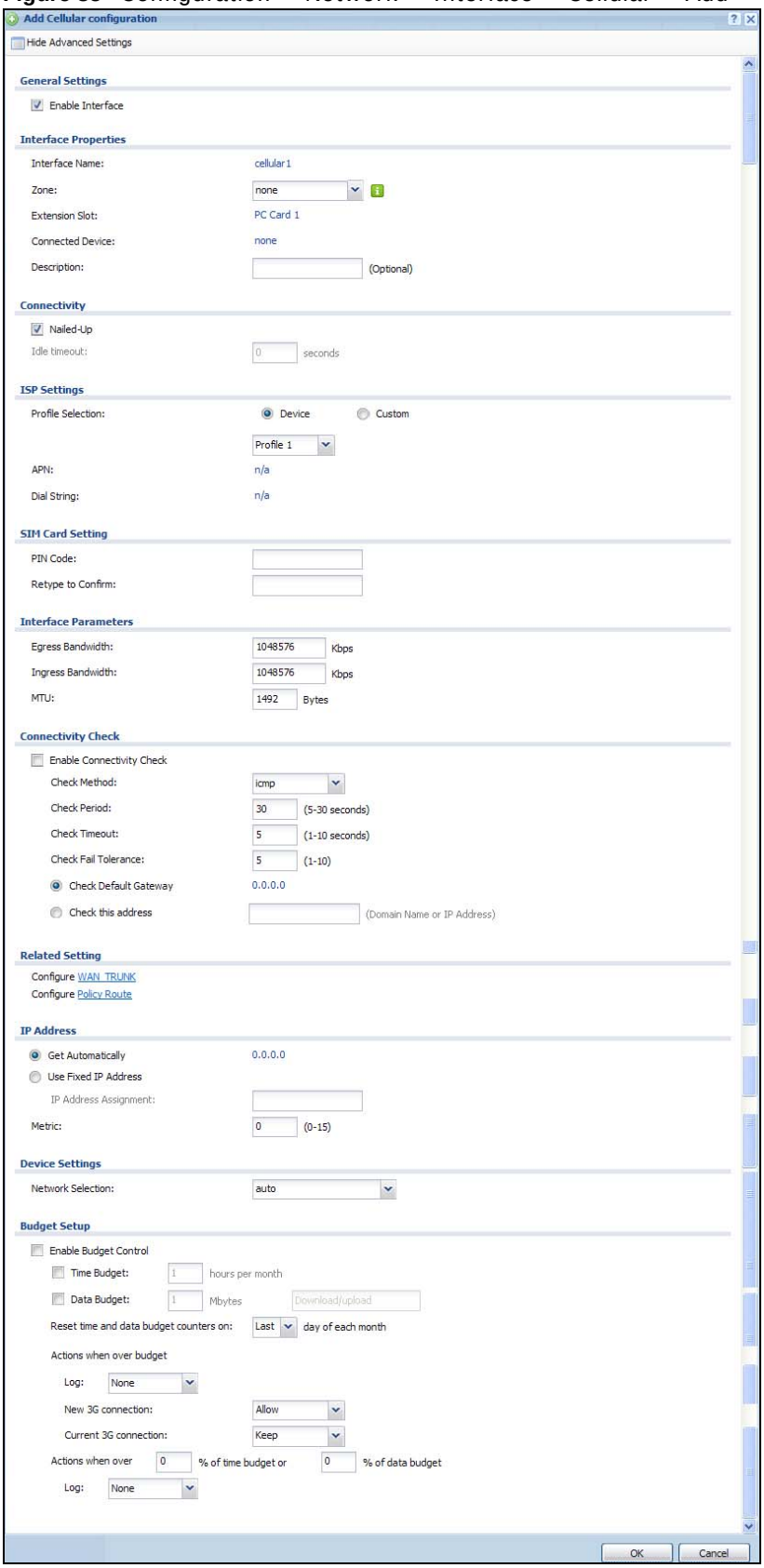
Table 48 Configuration > Network > Interface > Cellular

LABEL	DESCRIPTION
Add	Click this to create a new cellular interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the name of the cellular card.
ISP Settings	This field displays the profile of ISP settings that this cellular interface is set to use.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.5.1 Cellular Add/Edit Screen

To change your 3G settings, click **Configuration > Network > Interface** > **Cellular > Add** (or **Edit**). In the pop-up window that displays, select the slot that contains the 3G device, then the following screen displays.

Figure 85 Configuration > Network > Interface > Cellular > Add



The following table describes the labels in this screen.

Table 49 Configuration > Network > Interface > Cellular > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this option to turn on this interface.
Interface Properties	
Interface Name	Select a name for the interface.
Zone	Select the zone to which you want the cellular interface to belong. The zone determines the security settings the ZyWALL uses for the interface.
Extension Slot	This is the USB slot that you are configuring for use with a 3G card.
Connected Device	This displays the manufacturer and model name of your 3G card if you inserted one in the ZyWALL. Otherwise, it displays **none**.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the connection should always be up. Clear this to have the ZyWALL to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available.
Idle timeout	This value specifies the time in seconds (0~360) that elapses before the ZyWALL automatically disconnects from the ISP's server. Zero disables the idle timeout.
ISP Settings	
Profile Selection	Select **Device** to use one of the 3G device's profiles of device settings. Then select the profile (use **Profile 1** unless your ISP instructed you to do otherwise). Select **Custom** to configure your device settings yourself.
APN	This field is read-only if you selected **Device** in the profile selection. Select **Custom** in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA 3G card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 63 ASCII printable characters. Spaces are allowed.
Dial String	Enter the dial string if your ISP provides a string, which would include the APN, to initialize the 3G card. You can enter up to 63 ASCII printable characters. Spaces are allowed. This field is available only when you insert a GSM 3G card.
Authentication Type	The ZyWALL supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **None:** No authentication for outgoing calls. **CHAP** - Your ZyWALL accepts CHAP requests only. **PAP** - Your ZyWALL accepts PAP requests only.

Table 49 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
User Name	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection. If this field is configurable, enter the user name for this 3G card exactly as the service provider gave it to you. You can use 1 ~ 64 alphanumeric and #:%-_@$./ characters. The first character must be alphanumeric or -_@$./. Spaces are not allowed.
Password	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the 3G card's profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you. You can use 0 ~ 63 alphanumeric and `~!@#$%^&*()_-+={}|;:'<,>./ characters. Spaces are not allowed.
Retype to Confirm	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the 3G card's profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you.
SIM Card Setting	
PIN Code	This field displays with a GSM or HSDPA 3G card. A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number.
Retype to Confirm	Type the PIN code again to confirm it.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.

Table 49 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the policy route summary screen where you can configure a policy route to override the default routing and SNAT behavior for the interface.
IP Address Assignment	
Get Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address Assignment	Enter the cellular interface's WAN IP address in this field if you selected **Use Fixed IP Address**.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Device Settings	
Network Selection	This field appears if you selected a 3G device that allows you to select the type of network to use. Select the type of 3G service for your 3G connection. If you are unsure what to select, check with your 3G service provider to find the 3G service available to you in your region. Select **auto** to have the card connect to an available network. Choose this option if you do not know what networks are available. You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you. Select **GPRS / EDGE (GSM) only** to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the ZyWALL does not spend time looking for a WCDMA network. Select **UMTS / HSDPA (WCDMA) only** to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network.

Table 49 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Network Selection	Home network is the network to which you are originally subscribed. Select **Home** to have the 3G device connect only to the home network. If the home network is down, the ZyWALL's 3G Internet connection is also unavailable. Select **Auto** (Default) to allow the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
Budget Setup	
Enable Budget Control	Select this to set a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The ZyWALL takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the ZyWALL resets the statistics.
Data Budget	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. Select **Download** to set a limit on the downstream traffic (from the ISP to the ZyWALL). Select **Upload** to set a limit on the upstream traffic (from the ZyWALL to the ISP). Select **Download / Upload** to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the ZyWALL resets the statistics.
Reset time and data budget counters on	Select the date on which the ZyWALL resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the ZyWALL resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions when over budget	Specify the actions the ZyWALL takes when the time or data limit is exceeded.
Log	Select **None** to not create a log, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the ZyWALL send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
New 3G connection	Select **Allow** to permit new 3G connections or **Disallow** to drop/block new 3G connections.
Current 3G connection	Select **Keep** to maintain an existing 3G connection or **Drop** to disconnect it. You cannot set **New 3G connection** to **Allow** and **Current 3G connection** to **Drop** at the same time. If you set **New 3G connection** to **Disallow** and **Current 3G connection** to **Keep**, the ZyWALL allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
Actions when over % of time budget or % of data budget	Specify the actions the ZyWALL takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the ZyWALL resets the statistics.

Table 49 Configuration > Network > Interface > Cellular > Add (continued)

LABEL	DESCRIPTION
Log	Select **None** to not create a log when the ZyWALL takes this action, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the ZyWALL send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

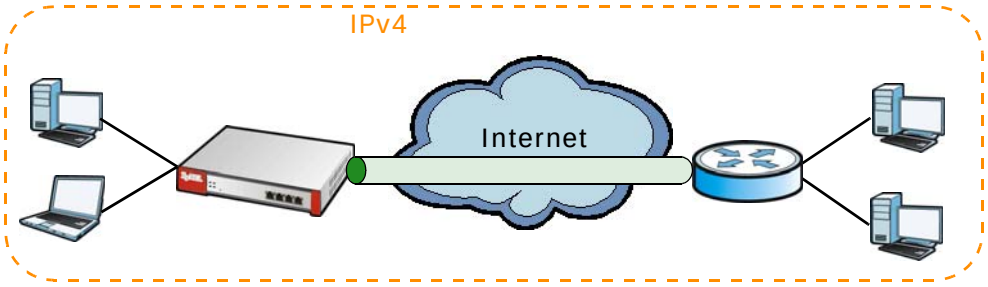
7.6 Tunnel Interfaces

The ZyWALL uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.

GRE Tunneling

GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the ZyWALL and another router over an IPv4 network. At the time of writing, the ZyWALL only supports GRE tunneling in IPv4 networks.

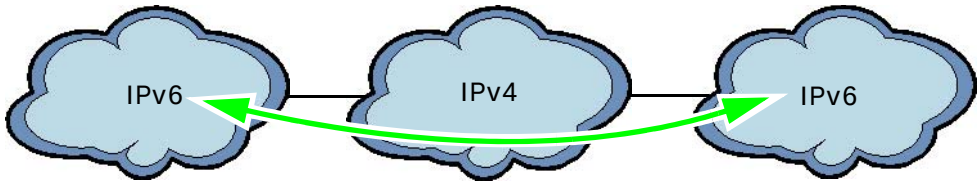
Figure 86 GRE Tunnel Example



IPv6 Over IPv4 Tunnels

To route traffic between two IPv6 networks over an IPv4 network, an IPv6 over IPv4 tunnel has to be used.

Figure 87 IPv6 over IPv4 Network



On the ZyWALL, you can either set up a manual IPv6-in-IPv4 tunnel or an automatic 6to4 tunnel. The following describes each method:

IPv6-in-IPv4 Tunneling

Use this mode on the WAN of the ZyWALL if

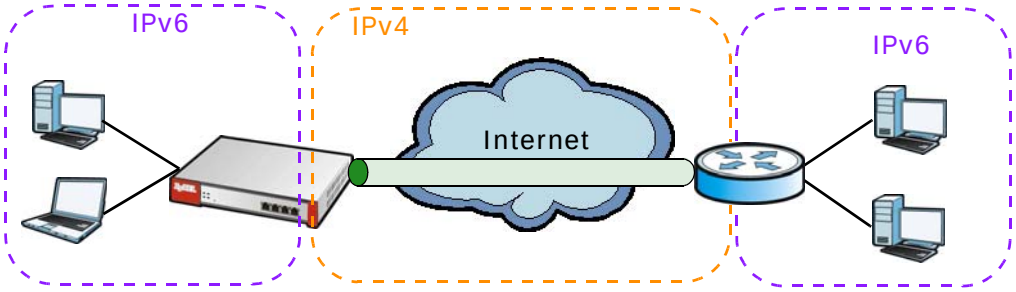
- your ZyWALL has a public IPv4 IP address given from your ISP,

and

- you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network.

With this mode, the ZyWALL encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.

Figure 88 IPv6-in-IPv4 Tunnel



In the ZyWALL, you must also manually configure a policy route for an IPv6-in-IPv4 tunnel to make the tunnel work.

6to4 Tunneling

This mode also enables IPv6 packets to cross IPv4 networks. Unlike IPv6-in-IPv4 tunneling, you do not need to configure a policy route for a 6to4 tunnel. Through your properly pre-configuring the destination router's IP address in the IP address assignments to hosts, the ZyWALL can automatically forward 6to4 packets to the destination they want to go. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network if the packet's destination do not match your specified criteria.

In this mode, the ZyWALL should get a public IPv4 address for the WAN. The ZyWALL adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the ZyWALL removes the IPv4 header from an IPv6 packet when receiving it from the Internet.

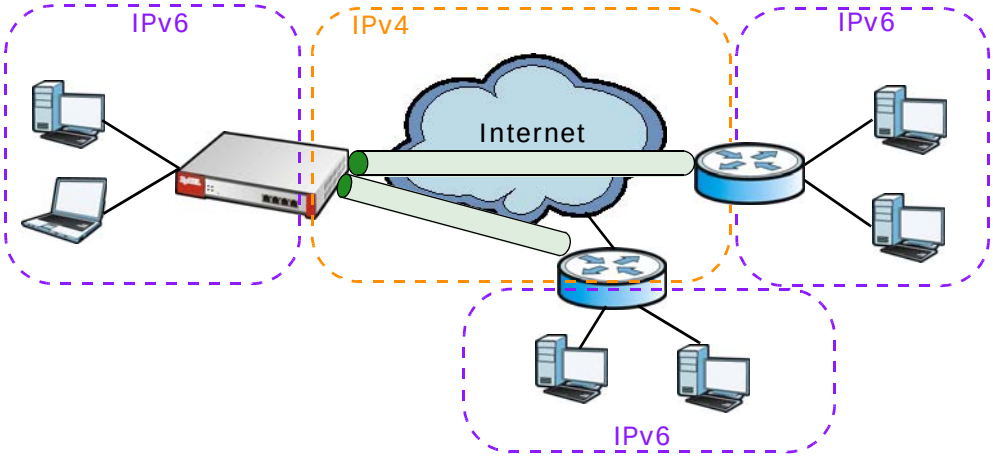
An IPv6 address using the 6to4 mode consists of an IPv4 address, the format is as the following:

2002:[a public IPv4 address in hexadecimal]::/48

For example,

A public IPv4 address is 202.156.30.41. The converted hexadecimal IP string is ca.9c.1E.29. The IPv6 address prefix becomes 2002:ca9c:1e29::/48.

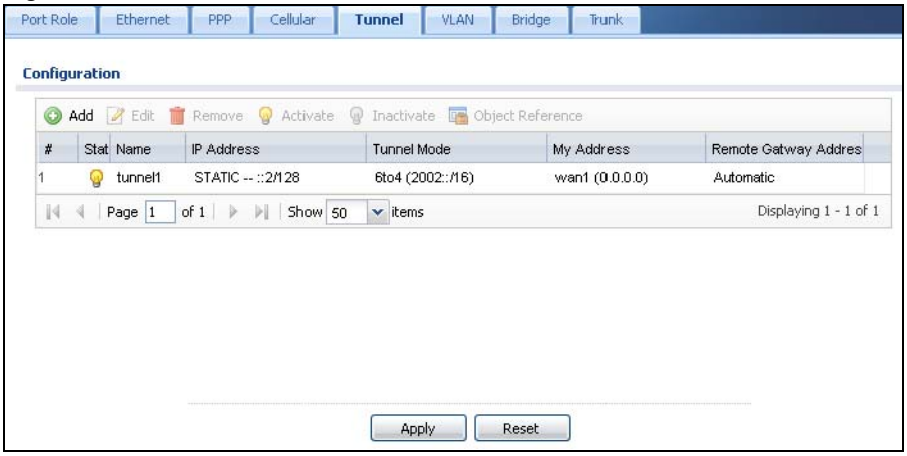
Figure 89 6to4 Tunnel



7.6.1 Configuring a Tunnel

This screen lists the ZyWALL's configured tunnel interfaces. To access this screen, click **Network** > **Interface** > **Tunnel**.

Figure 90 Network > Interface > Tunnel



Each field is explained in the following table.

Table 50 Network > Interface > Tunnel

LABEL	DESCRIPTION
Add	Click this to create a new GRE tunnel interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.

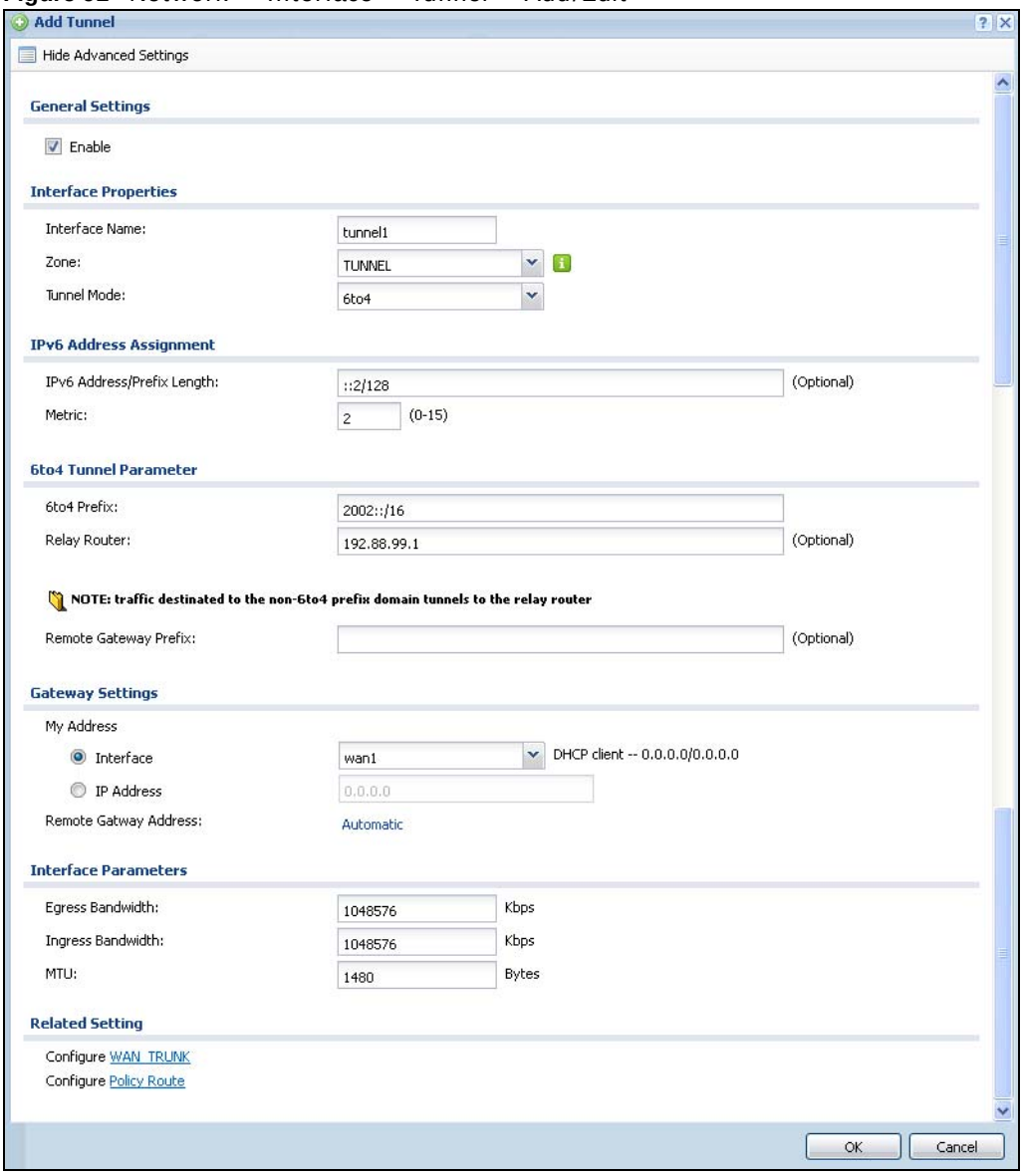
Table 50 Network > Interface > Tunnel (continued)

LABEL	DESCRIPTION
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This is the IP address of the interface. If the interface is active (and connected), the ZyWALL tunnels local traffic sent to this IP address to the **Remote Gateway Address**.
Tunnel Mode	This is the tunnel mode of the interface (**GRE**, **IPv6-in-IPv4** or **6to4**). This field also displays the interface's IPv4 IP address and subnet mask if it is a GRE tunnel. Otherwise, it displays the interface's IPv6 IP address and prefix length.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The ZyWALL uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

7.6.2 Tunnel Add or Edit Screen

This screen lets you configure a tunnel interface. Click **Configuration > Network > Interface > Tunnel > Add** (or **Edit**) to open the following screen.

Figure 91 Network > Interface > Tunnel > Add/Edit



Each field is explained in the following table.

Table 51 Network > Interface > Tunnel > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Name	This field is read-only if you are editing an existing tunnel interface. Enter the name of the tunnel interface. The format is tunnel*x*, where *x* is 0 - 3. For example, tunnel0.
Zone	Use this field to select the zone to which this interface belongs. This controls what security settings the ZyWALL applies to this interface.

Table 51 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Tunnel Mode	Select the tunneling protocol of the interface (**GRE**, **IPv6-in-IPv4** or **6to4**). See Section 7.6 on page 140 for more information.
IP Address Assignment	This section is available if you are configuring a GRE tunnel.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
IPv6 Address Assignment	This section is available if you are configuring an IPv6-in-IPv4 or a 6to4 tunnel.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
6to4 Tunnel Parameter	This section is available if you are configuring a 6to4 tunnel which encapsulates IPv6 to IPv4 packets.
6to4 Prefix	Enter the IPv6 prefix of a destination network. The ZyWALL forwards IPv6 packets to the hosts in the matched network. If you enter a prefix starting with 2002, the ZyWALL will forward the matched packets to the IPv4 IP address converted from the packets' destination address. The IPv4 IP address can be converted from the next 32 bits after the prefix you specified in this field. See 6to4 Tunneling on page 141 for an example. The ZyWALL forwards the unmatched packets to the specified **Relay Router**.
Relay Router	Enter the IPv4 address of a 6to4 relay router which helps forward packets between 6to4 networks and native IPv6 networks.
Remote Gateway Prefix	Enter the IPv4 network address and network bits of a remote 6to4 gateway, for example, 14.15.0.0/16. This field works if you enter a **6to4 Prefix** not starting with 2002 (2003 for example). The ZyWALL forwards the matched packets to a remote gateway with the network address you specify here, and the bits converted after the **6to4 Prefix** in the packets. For example, you configure the 6to4 prefix to 2003:A0B::/32 and the remote gateway prefix to 14.15.0.0/16. If a packet's destination is 2003:A0B:1011:5::8, the ZyWALL forwards the packet to 14.15.16.17, where the network address is 14.15.0.0 and the host address is the remain bits converted from 1011 after the packet's 6to4 prefix (2003:A0B).
Gateway Settings	
My Address	Specify the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. The remote gateway sends traffic to this interface or IP address.
Remote Gateway Address	Enter the IP address or domain name of the remote gateway to which this interface tunnels traffic. **Automatic** displays in this field if you are configuring a **6to4** tunnel. It means the 6to4 tunnel will help forward packets to the corresponding remote gateway automatically by looking at the packet's destination address.

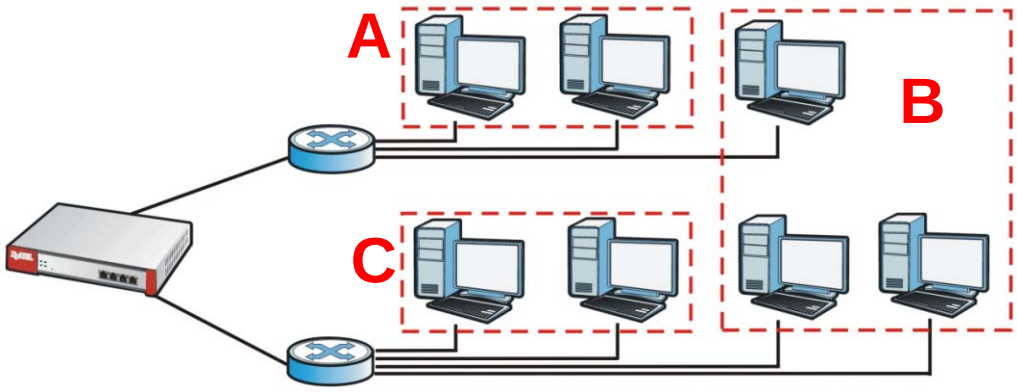
Table 51 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	This section is available if you are configuring a GRE tunnel. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
WAN TRUNK	Click this link to go to a screen where you can configure WAN trunk load balancing.
Policy Route	Click this link to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.7 VLAN Interfaces

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

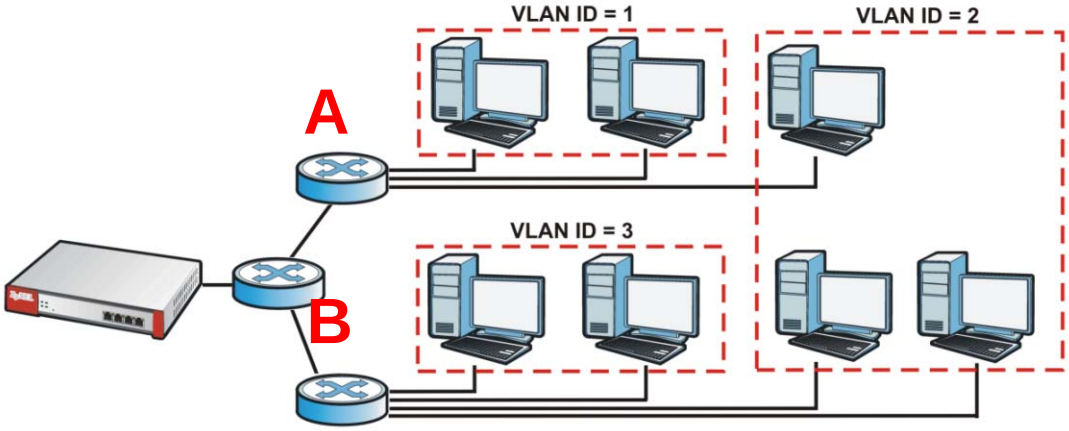
Figure 92 Example: Before VLAN



In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

Figure 93 Example: After VLAN



Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

VLAN Interfaces Overview

In the ZyWALL, each VLAN is called a VLAN interface. As a router, the ZyWALL routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

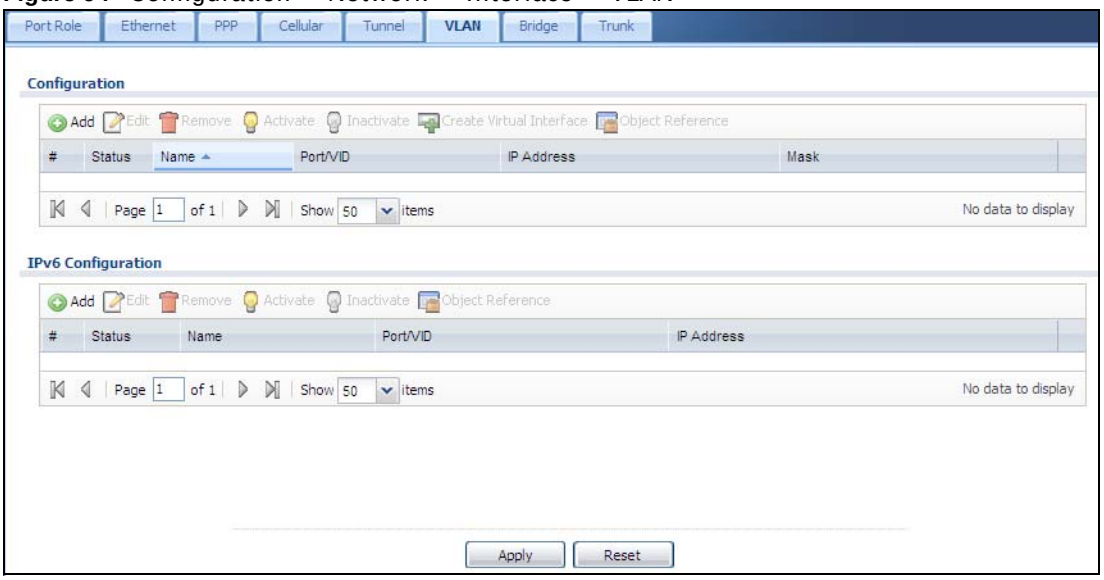
Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

7.7.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure VLAN interfaces used for your IPv6 networks on this screen. To access this screen, click **Configuration > Network > Interface** > **VLAN**.

Figure 94 Configuration > Network > Interface > VLAN



Each field is explained in the following table.

Table 52 Configuration > Network > Interface > VLAN

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your ZyWALL to an IPv6 network. Both sections have similar fields as described below.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.

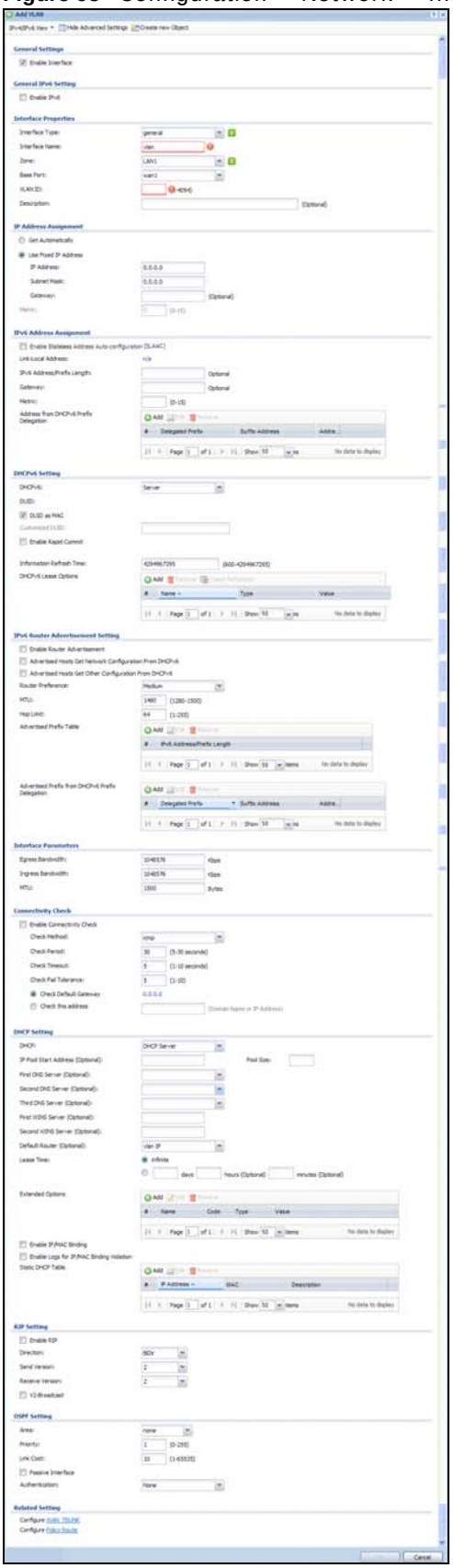
Table 52 Configuration > Network > Interface > VLAN (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.7.2 VLAN Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each VLAN interface. To access this screen, click the **Create Virtual Interface** icon in the **VLAN Summary** screen. The following screen appears.

Figure 95 Configuration > Network > Interface > VLAN > Create Virtual Interface



Each field is explained in the following table.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the ZyWALL is connected or if you want to additionally manually configure some related settings. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The ZyWALL automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. For example, vlan0, vlan8, and so on. The total number of VLANs you can configure on the ZyWALL depends on the model.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the ZyWALL generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to configure a static IP address for this interface. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the ZyWALL obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 107 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 107 for more information.
DUID as MAC	Select this to have the DUID generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If this interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 7.3.3 on page 123 for more information.
Remove	Select an entry and click this to change the settings.
Object Reference	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the ZyWALL obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 107 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DNS information is not available in this network.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the ZyWALL. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the ZyWALL to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The ZyWALL will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	The ZyWALL can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
DHCP Setting	The DHCP settings are available for the OPT, LAN and DMZ interfaces.
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 7.3.4 on page 124.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
Enable IP/MAC Binding	Select this option to have the ZyWALL enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ZyWALL generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ZyWALL assigns to computers connected to the interface. Otherwise, the ZyWALL assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.2 on page 199 for more information about RIP.
Enable RIP	Select this to enable RIP on this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting.
OSPF Setting	See Section 10.3 on page 201 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.

Table 53 Configuration > Network > Interface > VLAN > Create Virtual Interface (continued)

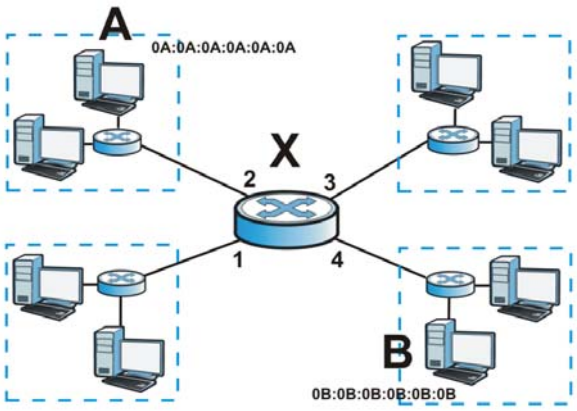
LABEL	DESCRIPTION
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.8 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 54 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 55 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2
0B:0B:0B:0B:0B:0B	4

Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the ZyWALL's interface for the resulting network.

Unlike the device-wide bridge mode in ZyNOS-based ZyWALLs, this ZyWALL can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole ZyWALL as a transparent bridge, add all of the ZyWALL's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the ZyWALL removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

Table 56 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1
210.211.1.0/24	lan1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	wan
241.241.241.241/32	dmz
242.242.242.242/32	dmz

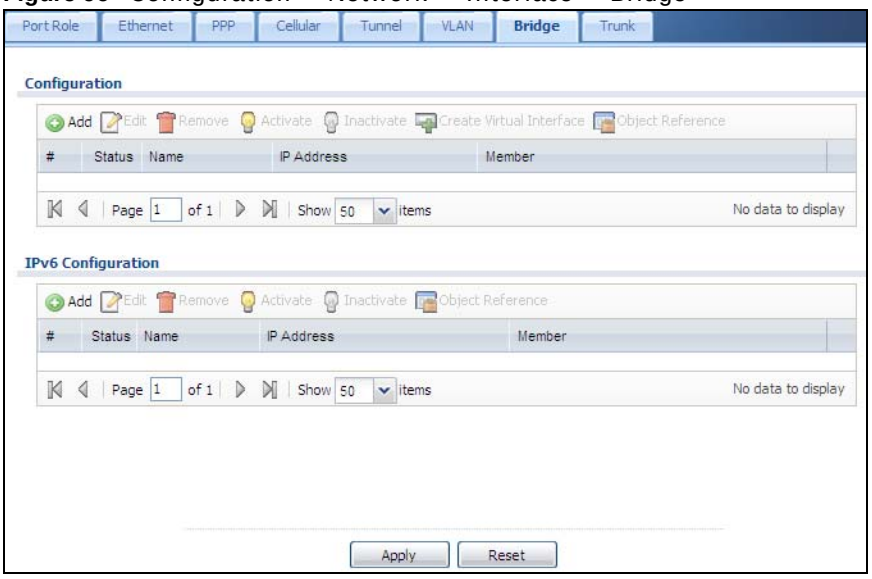
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	wan
241.241.241.241/32	dmz
242.242.242.242/32	dmz
250.250.250.0/23	br0

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

7.8.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure bridge interfaces used for your IPv6 network on this screen. To access this screen, click **Configuration** > **Network** > **Interface** > **Bridge**.

Figure 96 Configuration > Network > Interface > Bridge



Each field is described in the following table.

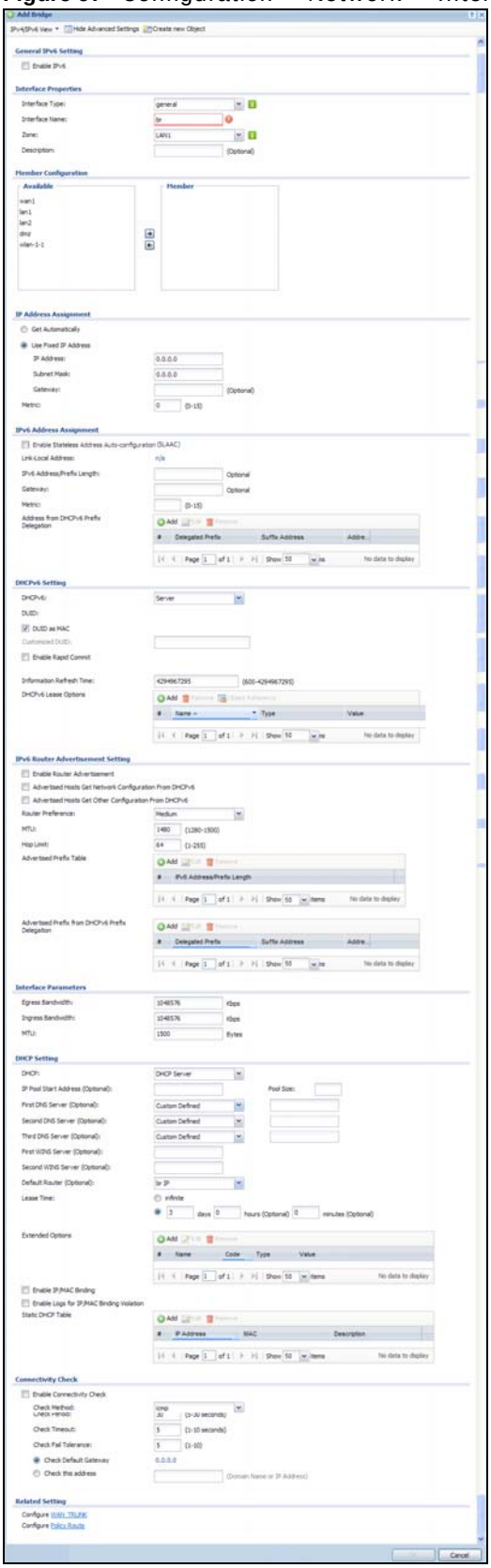
Table 57 Configuration > Network > Interface > Bridge

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your ZyWALL to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.
Object References	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

7.8.2 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each bridge interface. To access this screen, click the **Create Virtual Interface** icon in the **Bridge Summary** screen. The following screen appears.

Figure 97 Configuration > Network > Interface > Bridge > Create Virtual Interface



Each field is described in the table below.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the ZyWALL is connected or if you want to additionally manually configure some related settings. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The ZyWALL automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as firewall, remote management.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the **>>** arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the **<<** arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the ZyWALL generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the ZyWALL obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 107 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 107 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 7.3.3 on page 123 for more information.
Remove	Select an entry and click this to change the settings.
Object Reference	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the ZyWALL obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 107 for more information.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the ZyWALL indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the ZyWALL indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the ZyWALL. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the ZyWALL to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The ZyWALL will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Address	This is the final network prefix combined by the selected delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	
DHCP	Select what type of DHCP service the ZyWALL provides to the network. Choices are: **None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 7.3.4 on page 124.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the ZyWALL assigns to computers connected to the interface. Otherwise, the ZyWALL assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.

Table 58 Configuration > Network > Interface > Bridge > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.9 Virtual Interfaces

Use virtual interfaces to tell the ZyWALL where to route packets. Virtual interfaces can also be used in VPN gateways (see Chapter 20 on page 281) and VRRP groups (see Chapter 26 on page 359).

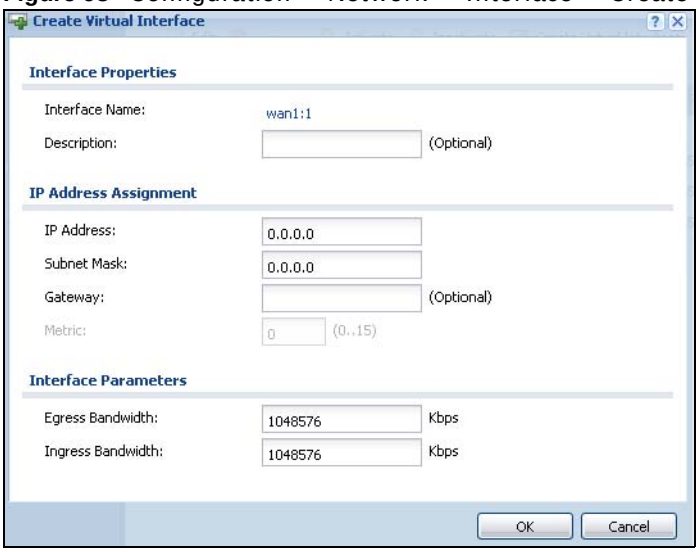
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, firewall rules) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

7.9.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click the **Create Virtual Interface** icon in the Ethernet, VLAN, or bridge interface summary screen.

Figure 98 Configuration > Network > Interface > Create Virtual Interface



Each field is described in the table below.

Table 59 Configuration > Network > Interface > Create Virtual Interface

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.

Table 59 Configuration > Network > Interface > Create Virtual Interface (continued)

LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

7.10 Interface Technical Reference

Here is more detailed information about interfaces on the ZyWALL.

IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 99 Example: Entry in the Routing Table Derived from Interfaces

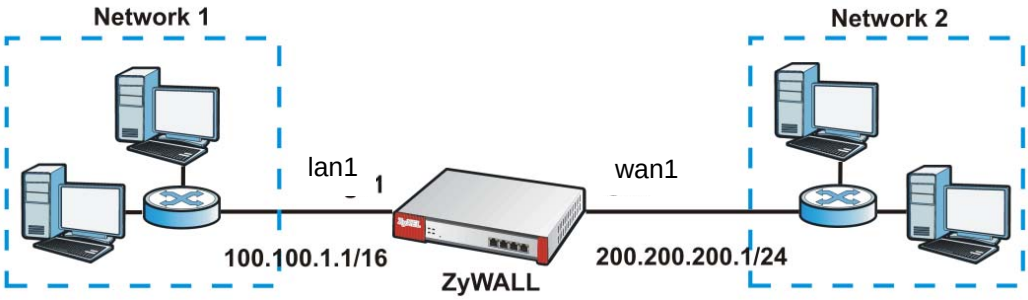


Table 60 Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	lan1
200.200.200.1/24	wan1

For example, if the ZyWALL gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the ZyWALL gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the ZyWALL gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the ZyWALL should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on ge2. In this case, the ZyWALL creates the following entry in the routing table.

Table 61 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the ZyWALL uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the ZyWALL uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

Interface Parameters

The ZyWALL restricts the amount of traffic into and out of the ZyWALL through each interface.

- Egress bandwidth sets the amount of traffic the ZyWALL sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the ZyWALL allows in through the interface from the network.[2]

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The ZyWALL also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the ZyWALL divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

2. At the time of writing, the ZyWALL does not support ingress bandwidth management.

In the ZyWALL, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ZyWALL's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 62 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

  The ZyWALL cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the ZyWALL cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the ZyWALL cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

  If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 172.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 172.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

1. The first one runs on TCP port 1723. It is used to start and manage the second one.
2. The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

8 Trunk

8.1 Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the ZyWALL's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

8.1.1 What You Can Do in this Chapter

- Use the **Trunk** summary screen (Section 8.2 on page 180) to configure link sticking and view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Add Trunk** screen (Section 8.2.1 on page 181) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the **Add System Default** screen (Section 8.2.2 on page 183) to configure the load balancing algorithm for the system default trunk.

8.1.2 What You Need to Know

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface's connection goes down, the ZyWALL sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The ZyWALL balances the WAN traffic load between the connections. If one interface's connection goes down, the ZyWALL can automatically send its traffic through another interface.

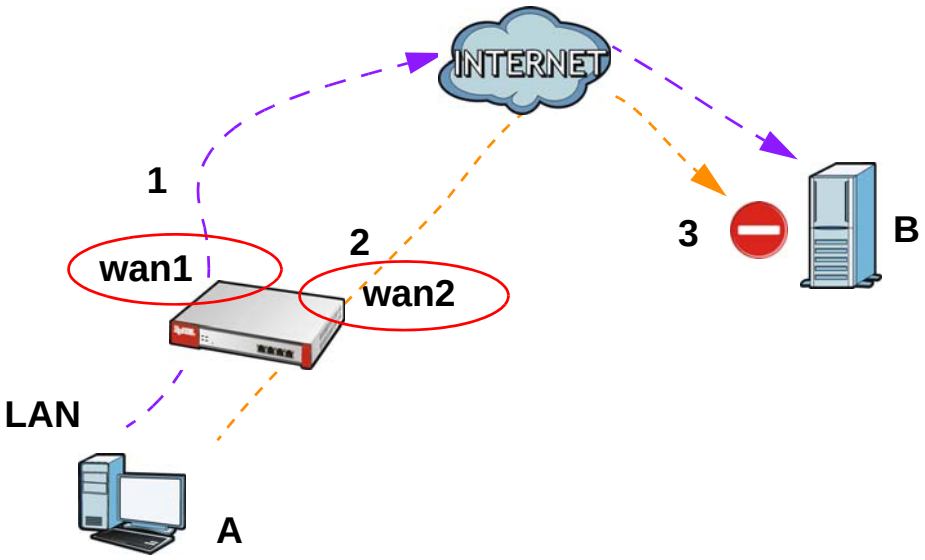
You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- If that interface's connection goes down, the ZyWALL can still send its traffic through another interface.
- You can define multiple trunks for the same physical interfaces.

Link Sticking

You can have the ZyWALL send each local computer's traffic that is going to the same destination through a single WAN interface for a specified period of time. This is useful when a server requires authentication. For example, the ZyWALL sends a user's traffic through one WAN IP address when he logs into a server B. If the user's subsequent sessions came from a different WAN IP address, the server would deny them. Here is an example.

Figure 100 Link Sticking



Load Balancing Algorithms

The following sections describe the load balancing algorithms the ZyWALL can use to decide which interface the traffic (from the LAN) should use for a session[3]. The available bandwidth you configure on the ZyWALL refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

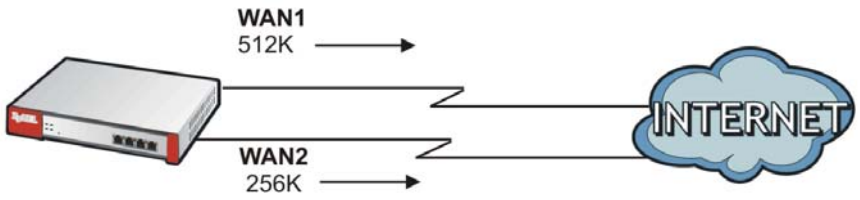
Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

Here the ZyWALL has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

3. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic.

Figure 101 Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The ZyWALL calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the ZyWALL will send the subsequent new session traffic through WAN 2.

Table 63 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

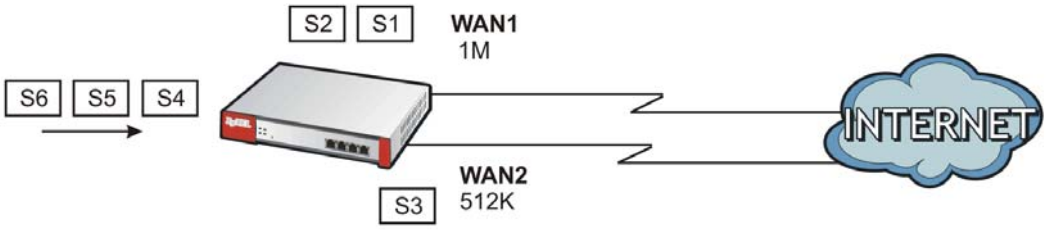
Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the ZyWALL to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the ZyWALL to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The ZyWALL assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 102 Weighted Round Robin Algorithm Example

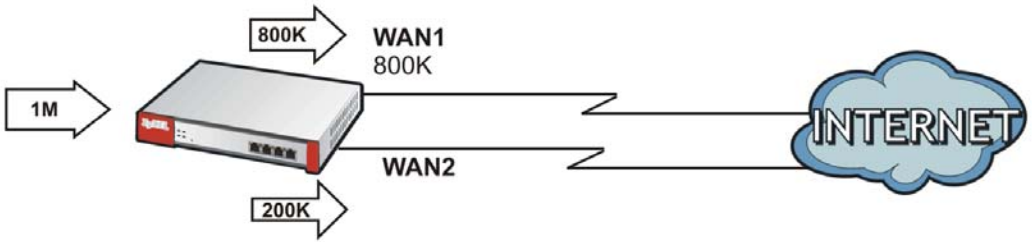


Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

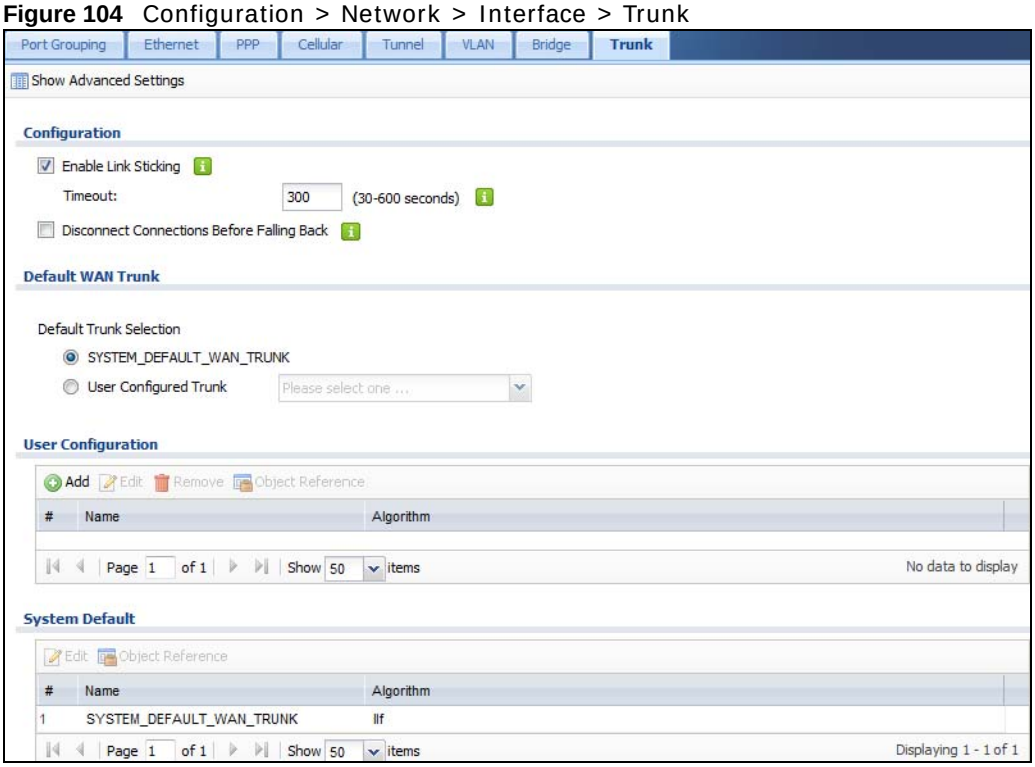
Figure 103 Spillover Algorithm Example



8.2 The Trunk Summary Screen

Click **Configuration > Network > Interface > Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 104 Configuration > Network > Interface > Trunk



The following table describes the items in this screen.

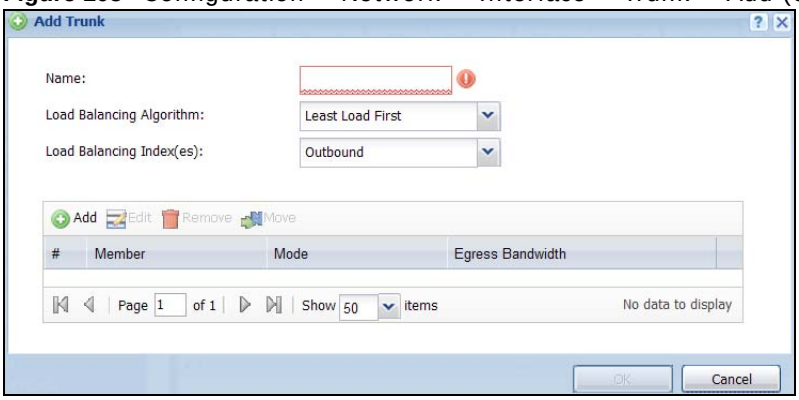
Table 64 Configuration > Network > Interface > Trunk

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable Link Sticking	Enable link sticking to have the system route sessions from one source to the same destination through the same link for a period of time. This is useful for accessing server that are incompatible with a user's sessions coming from different links. For example, this is useful when a server requires authentication. This setting applies when you use load balancing and have multiple WAN interfaces set to active mode.
Timeout	Specify the time period during which sessions from one source to the same destination are to use the same link.
Disconnect Connections Before Falling Back	Select this to terminate existing connections on an interface which is set to passive mode when any interface set to active mode in the same trunk comes back up.
Enable Default SNAT	Select this to have the ZyWALL use the IP address of the outgoing interface as the source IP address of the packets it sends out through its WAN trunks. The ZyWALL automatically adds SNAT settings for traffic it routes from internal interfaces to external interfaces.
Default Trunk Selection	Select whether the ZyWALL is to use the default system WAN trunk or one of the user configured WAN trunks as the default trunk for routing traffic from internal interfaces to external interfaces.
User Configuration / System Default	The ZyWALL automatically adds all external interfaces into the pre-configured system default **SYSTEM_DEFAULT_WAN_TRUNK**. You cannot delete it. You can create your own **User Configuration** trunks and customize the algorithm, member interfaces and the active/passive mode.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

8.2.1 Configuring a User-Defined Trunk

Click **Configuration > Network > Interface > Trunk**, in the **User Configuration** table click the **Add** (or **Edit**) icon to open the **following** screen. Use this screen to create or edit a WAN trunk entry.

Figure 105 Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 65 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the ZyWALL chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
Load Balancing Index(es)	This field is available if you selected to use the **Least Load First** or **Spillover** method. Select **Outbound**, **Inbound**, or **Outbound + Inbound** to set the traffic to which the ZyWALL applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click **Add** to add a new member interface after the selected member interface.
Edit	Select an entry and click **Edit** to modify the entry's settings.
Remove	To remove a member interface, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Move	To move an interface to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.

Table 65 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

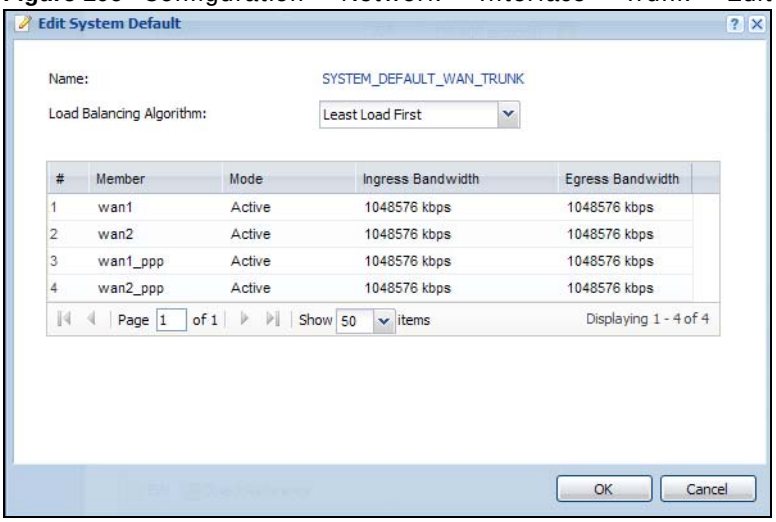
LABEL	DESCRIPTION
Member	Click this table cell and select an interface to be a group member. If you select an interface that is part of another Ethernet interface, the ZyWALL does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the ZyWALL will not send traffic through port 5 as part of the trunk.
Mode	Click this table cell and select **Active** to have the ZyWALL always attempt to use this connection. Select **Passive** to have the ZyWALL only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the ZyWALL assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to allow to come in through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to send out through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ZyWALL sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The ZyWALL uses the group member interfaces in the order that they are listed.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

8.2.2 Configuring the System Default Trunk

In the **Configuration > Network > Interface > Trunk** screen and the **System Default** section, select the default trunk entry and click **Edit** to open the **following** screen. Use this screen to change the load balancing algorithm and view the bandwidth allocations for each member interface.

Note: The available bandwidth is allocated to each member interface equally and is not allowed to be changed for the default trunk.

Figure 106 Configuration > Network > Interface > Trunk > Edit (System Default)


Edit System Default
Name:
SYSTEM_DEFAULT_WAN_TRUNK
Load Balancing Algorithm:
Least Load First
Member Mode Ingress Bandwidth Egress Bandwidth
1 wan1 Active 1048576 kbps 1048576 kbps
2 wan2 Active 1048576 kbps 1048576 kbps
3 wan1_ppp Active 1048576 kbps 1048576 kbps
4 wan2_ppp Active 1048576 kbps 1048576 kbps
Page 1 of 1 Show 50 items
Displaying 1 - 4 of 4
OK
Cancel

Each field is described in the table below.

Table 66 Configuration > Network > Interface > Trunk > Edit (System Default)

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Algorithm	Select the load balancing method to use for the trunk. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the ZyWALL chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
	The table lists the trunk's member interfaces. This table is read-only.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	This column displays the name of the member interfaces.
Mode	This field displays **Active** if the ZyWALL always attempt to use this connection. This field displays **Passive** if the ZyWALL only use this connection when all of the connections set to active are down. Only one of a group's interfaces can be set to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. s
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to allow to come in through the interface per second.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to send out through the interface per second.

Table 66 Configuration > Network > Interface > Trunk > Edit (System Default) (continued)

LABEL	DESCRIPTION
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ZyWALL sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The ZyWALL uses the group member interfaces in the order that they are listed.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

9

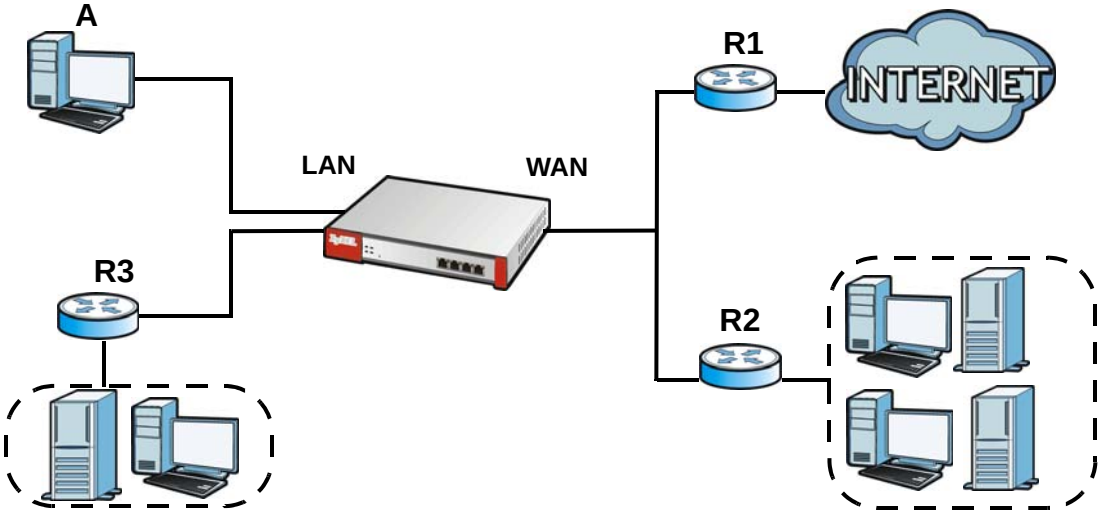
Policy and Static Routes

9.1 Policy and Static Routes Overview

Use policy routes and static routes to override the ZyWALL's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

For example, the next figure shows a computer (**A**) connected to the ZyWALL's LAN interface. The ZyWALL routes most traffic from **A** to the Internet through the ZyWALL's default gateway (**R1**). You create one policy route to connect to services offered by your ISP behind router **R2**. You create another policy route to communicate with a separate network behind another router (**R3**) connected to the LAN.

Figure 107 Example of Policy Routing Topology



Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

9.1.1 What You Can Do in this Chapter

- Use the **Policy Route** screens (see Section 9.2 on page 189) to list and configure policy routes.
- Use the **Static Route** screens (see Section 9.3 on page 195) to list and configure static routes.

9.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic. You can also use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyWALL performs NAT by default for traffic going to or from the **WAN** interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

Note: The ZyWALL automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic.

Static Routes

The ZyWALL usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyWALL send data to devices not reachable through the default gateway, use static routes. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 10 on page 199 for more on RIP and OSPF.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the ZyWALL itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the ZyWALL and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP Marking and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP (6 bits)	Unused (2 bits)

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Finding Out More

- See Section 9.4 on page 197 for more background information on policy routing.

9.2 Policy Route Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

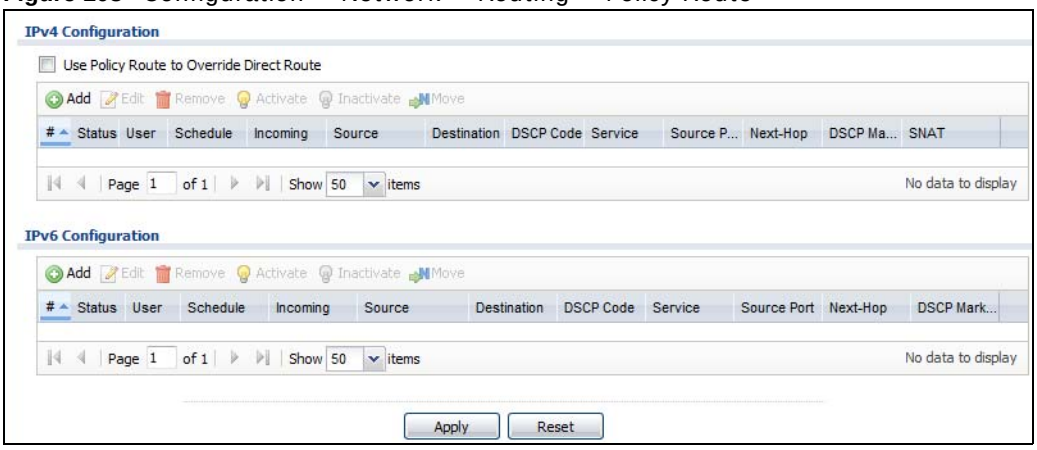
The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure policy routes used for your IPv6 networks on this screen.

Figure 108 Configuration > Network > Routing > Policy Route


IPv4 Configuration
Use Policy Route to Override Direct Route
Add Edit Remove Activate Inactivate Move
Status User Schedule Incoming Source Destination DSCP Code Service Source P... Next-Hop DSCP Ma... SNAT
Page 1 of 1 Show 50 items
No data to display
IPv6 Configuration
Add Edit Remove Activate Inactivate Move
Status User Schedule Incoming Source Destination DSCP Code Service Source Port Next-Hop DSCP Mark...
Page 1 of 1 Show 50 items
No data to display
Apply
Reset

The following table describes the labels in this screen.

Table 67 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
IPv4 Configuration / IPv6 Configuration	Use the **IPv4 Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your ZyWALL to an IPv6 network. Both sections have similar fields as described below.
Use Policy Route to Override Direct Route	Select this to have the ZyWALL forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This is the number of an individual policy route.
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users.
Schedule	This is the name of the schedule object. **none** means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object. **any** means all IP addresses.
Destination	This is the name of the destination IP address (group) object. **any** means all IP addresses.

Table 67 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. **any** means all DSCP values or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" entries stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 197 for more details.
Service	This is the name of the service object. **any** means all services.
Source Port	This is the name of a service object. The ZyWALL applies the policy route to the packets sent from the corresponding service port. **any** means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
DSCP Marking	This is how the ZyWALL handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the ZyWALL applies that DSCP value to the route's outgoing packets. **preserve** means the ZyWALL does not modify the DSCP value of the route's outgoing packets. **default** means the ZyWALL sets the DSCP value of the route's outgoing packets to 0. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 197 for more details.
SNAT	This is the source IP address that the route uses. It displays **none** if the ZyWALL does not perform NAT for this route.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

9.2.1 Policy Route Edit Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon in the **IPv4 Configuration** or **IPv6 Configuration** section. The **Add Policy Route** or **Policy Route Edit** screen opens. Use this screen to configure or edit a policy route. Both IPv4 and IPv6 policy route have similar settings except the **Address Translation** (SNAT) settings.

Figure 109 Configuration > Network > Routing > Policy Route > Add/Edit (IPv4 Configuration)

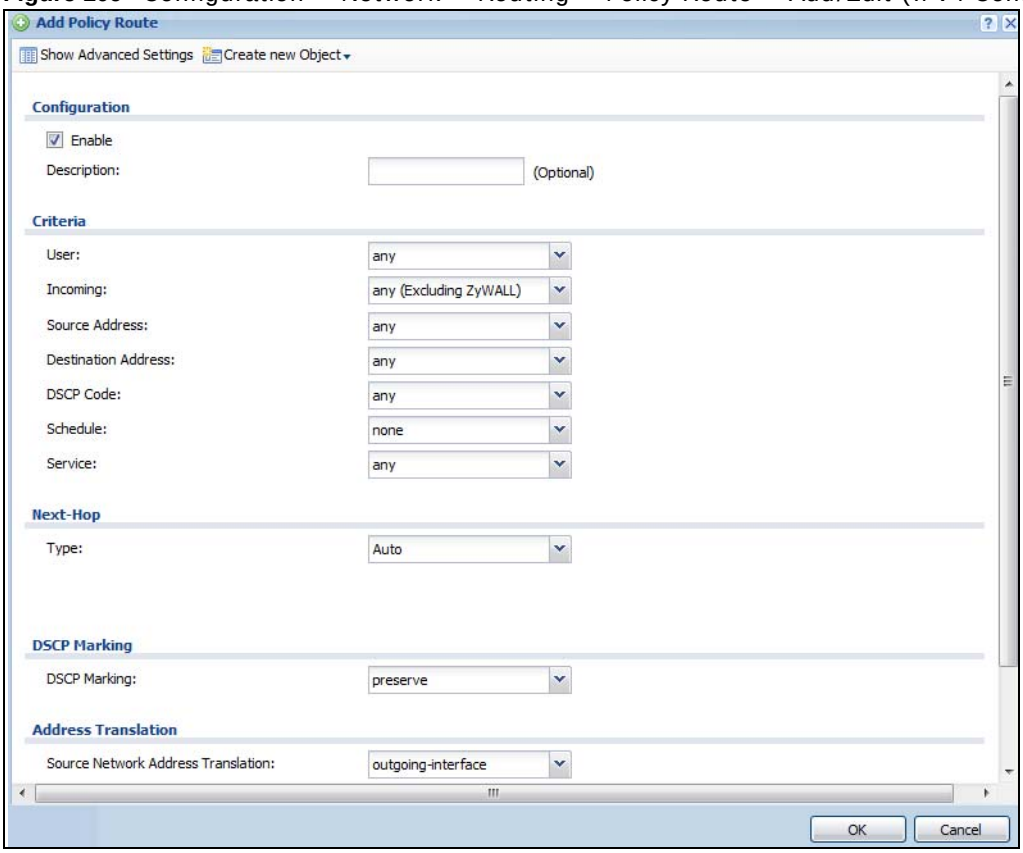
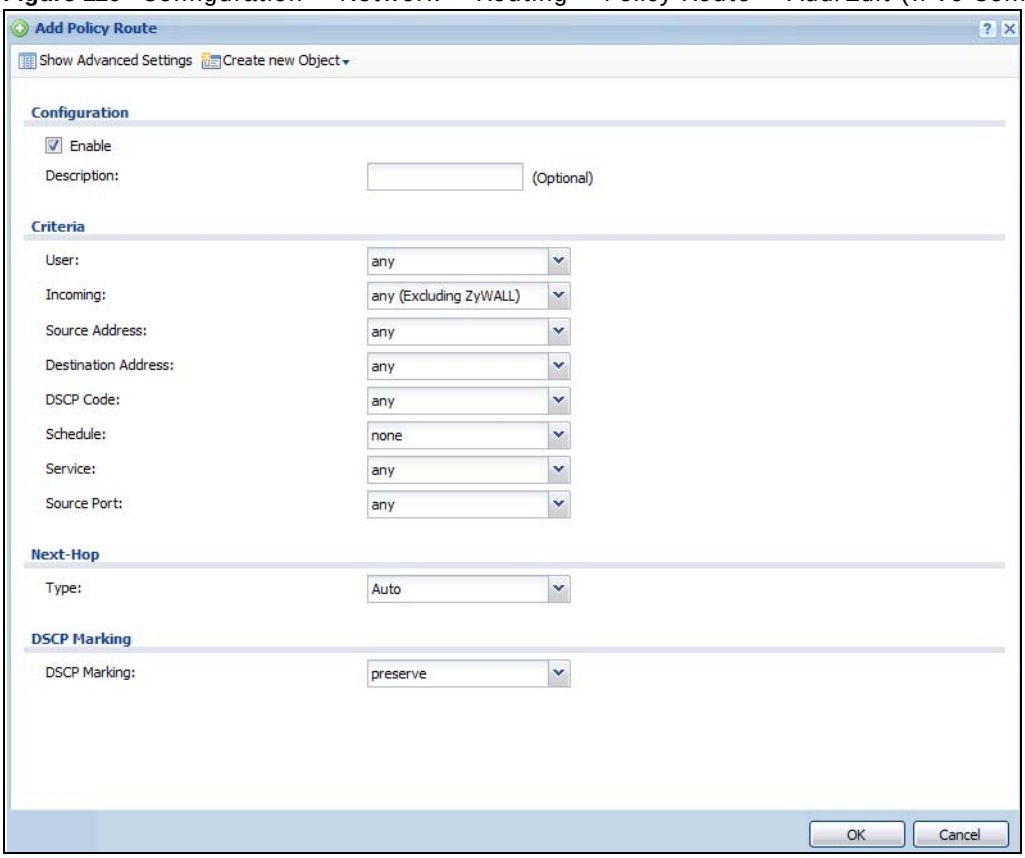


Figure 110 Configuration > Network > Routing > Policy Route > Add/Edit (IPv6 Configuration)



The following table describes the labels in this screen.

Table 68 Configuration > Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming	Select where the packets are coming from; any, an interface, a tunnel, an SSL VPN, or the ZyWALL itself. For an interface, a tunnel, or an SSL VPN, you also need to select the individual interface, VPN tunnel, or SSL VPN connection.
Source Address	Select a source IP address object from which the packets are sent.
Destination Address	Select a destination IP address object to which the traffic is being sent. If the next hop is a dynamic VPN tunnel and you enable **Auto Destination Address**, the ZyWALL uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.

Table 68 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select **User Define** to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 197 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Schedule	Select a schedule to control when the policy route is active. **none** means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	
Type	Select **Auto** to have the ZyWALL use the routing table to find a next-hop and forward the matched packets automatically. Select **Gateway** to route the matched packets to the next-hop router or switch you specified in the **Gateway** field. You have to set up the next-hop router or switch as a HOST address object first. Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel. Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select **Gateway** in the **Type** field. Select a HOST address object. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your ZyWALL's interface(s).
VPN Tunnel	This field displays when you select **VPN Tunnel** in the **Type** field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the ZyWALL directly.
Auto Destination Address	This field displays when you select **VPN Tunnel** in the **Type** field. Select this to have the ZyWALL use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy. Leave this cleared if you want to manually specify the destination address.
Trunk	This field displays when you select **Trunk** in the **Type** field. Select a trunk group to have the ZyWALL send the packets via the interfaces in the group.
Interface	This field displays when you select **Interface** in the **Type** field. Select an interface to have the ZyWALL send traffic that matches the policy route through the specified interface.
Auto-Disable	This field displays when you select **Interface** or **Trunk** in the **Type** field. Select this to have the ZyWALL automatically disable this policy route when the next hop's connection is down.

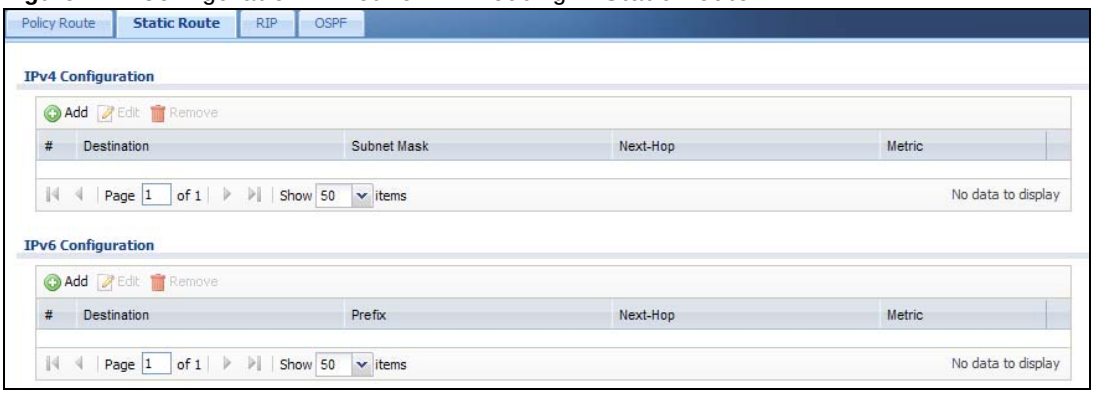
Table 68 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Marking	Set how the ZyWALL handles the DSCP value of the outgoing packets that match this route. Select one of the pre-defined DSCP values to apply or select **User Define** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 197 for more details. Select **preserve** to have the ZyWALL keep the packets' original DSCP value. Select **default** to have the ZyWALL set the DSCP value of the packets to 0.
User-Defined DSCP Code	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop.
Source Network Address Translation	Select **none** to not use NAT for the route. Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Use **Create new Object** if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

9.3 IP Static Route Screen

Click **Configuration > Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure static routes used for your IPv6 networks on this screen.

Figure 111 Configuration > Network > Routing > Static Route



The following table describes the labels in this screen.

Table 69 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
IPv4 Configuration / IPv6 Configuration	Use the **IPv4 Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your ZyWALL to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Prefix	This is the IPv6 prefix for the destination IP address.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.

9.3.1 Static Route Add/Edit Screen

Select a static route index number and click **Add** or **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 112 Configuration > Network > Routing > Static Route > Add (IPv4 Configuration)

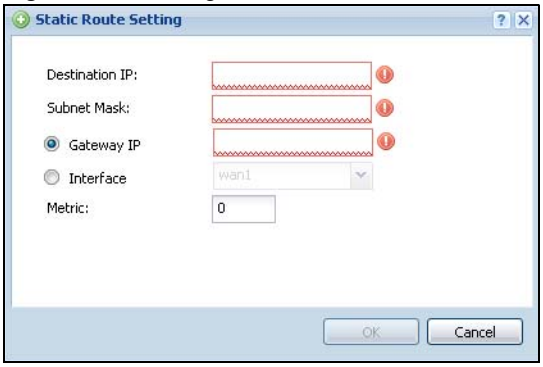
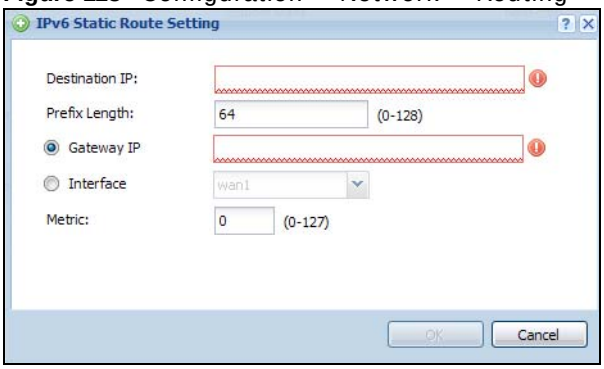


Figure 113 Configuration > Network > Routing > Static Route > Add (IPv6 Configuration)



The following table describes the labels in this screen.

Table 70 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, enter the specific IP address here and use a subnet mask of 255.255.255.255 (for IPv4) in the **Subnet Mask** field or a prefix of 128 (for IPv6) in the **Prefix Length** field to force the network number to be identical to the host ID. For IPv6, if you want to send all traffic to the gateway or interface specified in the **Gateway IP** or **Interface** field, enter :: in this field and 0 in the **Prefix Length** field.
Subnet Mask	Enter the IP subnet mask here.
Prefix Length	Enter the number of left-most digits in the destination IP address, which indicates the network prefix. Enter :: in the **Destination IP** field and 0 in this field if you want to send all traffic to the gateway or interface specified in the **Gateway IP** or **Interface** field.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

9.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces

the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 71 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

Maximize Bandwidth Usage

The maximize bandwidth usage option allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each policy route gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the policy routes) depending on how many policy routes require more bandwidth and on their priority levels. When only one policy route requires more bandwidth, the ZyWALL gives the extra bandwidth to that policy route.

When multiple policy routes require more bandwidth, the ZyWALL gives the highest priority policy routes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority policy routes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among policy routes with the same priority level.

10

Routing Protocols

10.1 Routing Protocols Overview

Routing protocols give the ZyWALL routing information about the network from other routers. The ZyWALL stores this routing information in the routing table it uses to make routing decisions. In turn, the ZyWALL can also use routing protocols to propagate routing information to other routers.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

10.1.1 What You Can Do in this Chapter

- Use the **RIP** screen (see Section 10.2 on page 199) to configure the ZyWALL to use RIP to receive and/or send routing information.
- Use the **OSPF** screen (see Section 10.3 on page 201) to configure general OSPF settings and manage OSPF areas.
- Use the **OSPF Area Add/Edit** screen (see Section 10.3.2 on page 206) to create or edit an OSPF area.

10.1.2 What You Need to Know

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

Table 72 RIP vs. OSPF

	RIP	OSPF
Network Size	Small (with up to 15 routers)	Large
Metric	Hop count	Bandwidth, hop count, throughput, round trip time and reliability.
Convergence	Slow	Fast

Finding Out More

See Section 10.4 on page 208 for background information on routing protocols.

10.2 The RIP Screen

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts

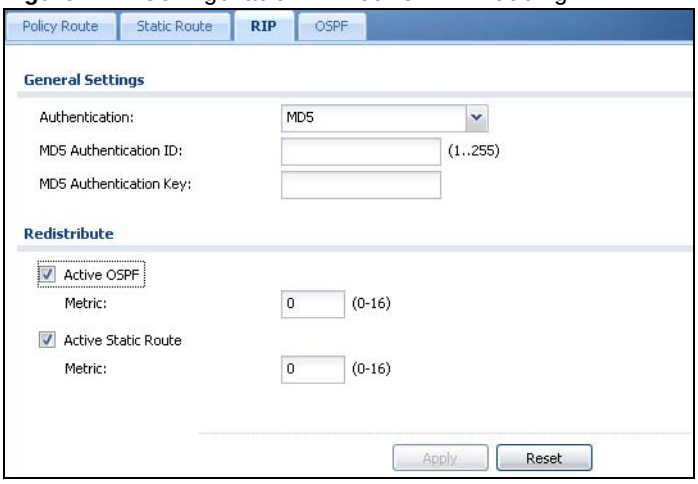
its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the ZyWALL, you can configure two sets of RIP settings before you can use it in an interface.
- First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in Authentication Types on page 209.
- Second, the ZyWALL can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the **RIP** screen to specify the authentication method and maintain the policies for redistribution.

Click **Configuration > Network** > **Routing > RIP** to open the following screen.

Figure 114 Configuration > Network > Routing > RIP



The following table describes the labels in this screen.

Table 73 Configuration > Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	
Authentication	Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.

Table 73 Configuration > Network > Routing Protocol > RIP (continued)

LABEL	DESCRIPTION
Redistribute	
Active OSPF	Select this to use RIP to advertise routes that were learned through OSPF.
Metric	Type the cost for routes provided by OSPF. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Active Static Route	Select this to use RIP to advertise routes that were learned through the static route configuration.
Metric	Type the cost for routes provided by the static route configuration. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

10.3 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

OSPF Areas

An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

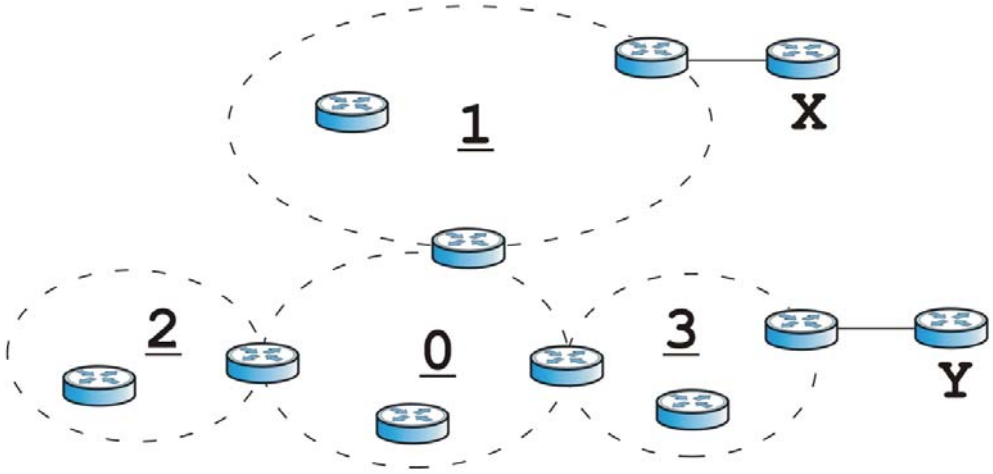
There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.

- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 115 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.

- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

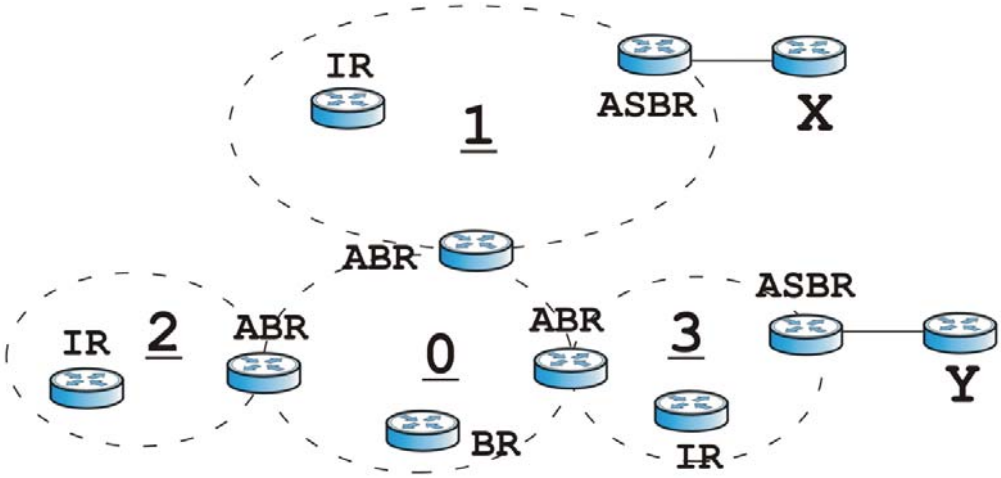
Table 74 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 116 OSPF: Types of Routers



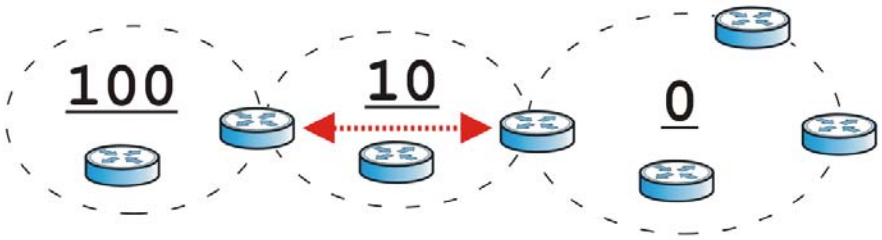
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 117 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

OSPF Configuration

Follow these steps when you configure OSPF on the ZyWALL.

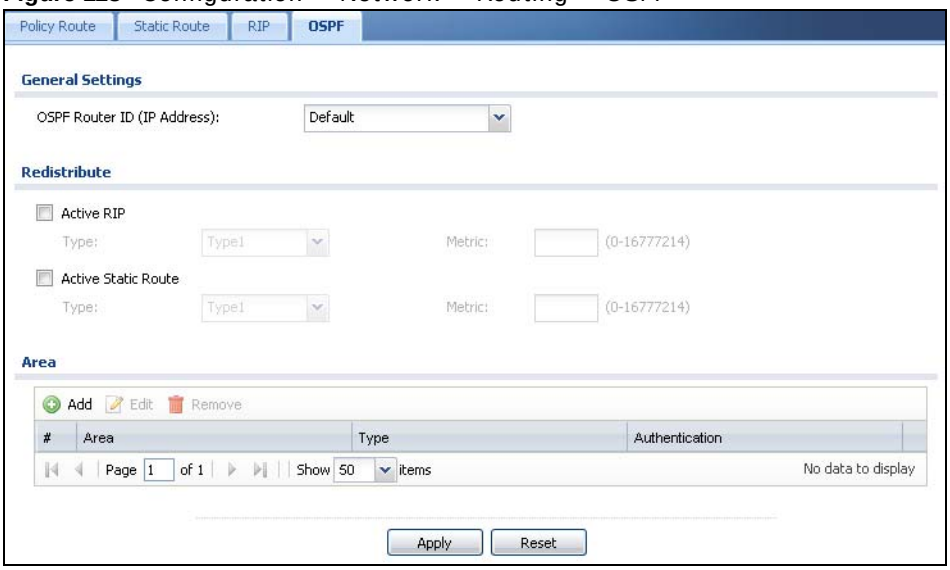
1. Enable OSPF.
2. Set up the OSPF areas.
3. Configure the appropriate interfaces. See Section 7.3.1 on page 110.
4. Set up virtual links, as needed.

10.3.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the ZyWALL uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add/Edit** screen to add or edit them.

Click **Configuration > Network** > **Routing > OSPF** to open the following screen.

Figure 118 Configuration > Network > Routing > OSPF



The following table describes the labels in this screen. See Section 10.3.2 on page 206 for more information as well.

Table 75 Configuration > Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the ZyWALL uses in the OSPF AS. **Default** - the first available interface IP address is the ZyWALL's ID. **User Defined** - enter the ID (in IP address format) in the field that appears when you select **User Define.**
Redistribute	
Active RIP	Select this to advertise routes that were learned from RIP. The ZyWALL advertises routes learned from RIP to **Normal** and **NSSA** areas but not to **Stub** areas.
Type	Select how OSPF calculates the cost associated with routing information from RIP. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by RIP. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Active Static Route	Select this to advertise routes that were learned from static routes. The ZyWALL advertises routes learned from static routes to all types of areas.
Type	Select how OSPF calculates the cost associated with routing information from static routes. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by static routes. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the ZyWALL.

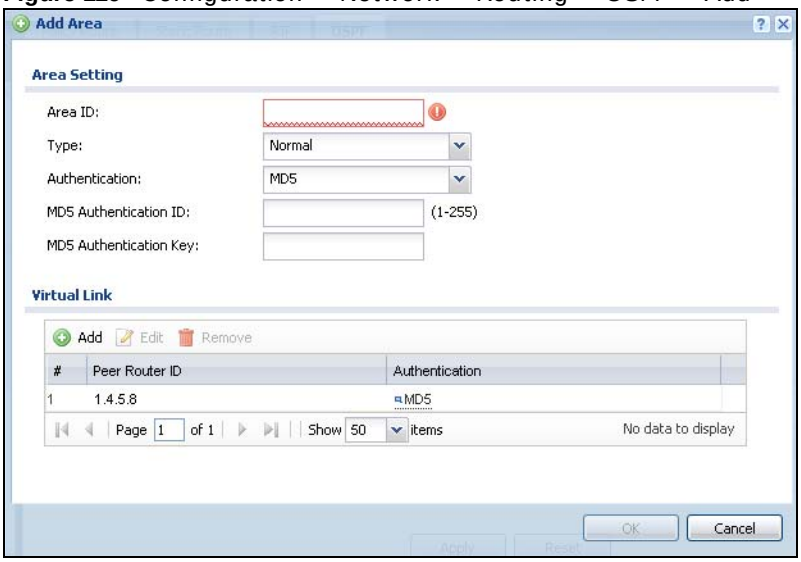
Table 75 Configuration > Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Add	Click this to create a new OSPF area.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the **Type** field above.
Authentication	This field displays the default authentication method in the area.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

10.3.2 OSPF Area Add/Edit Screen

The **OSPF Area Add / Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see Section 10.3 on page 201), and click either the **Add** icon or an **Edit** icon.

Figure 119 Configuration > Network > Routing > OSPF > Add



The following table describes the labels in this screen.

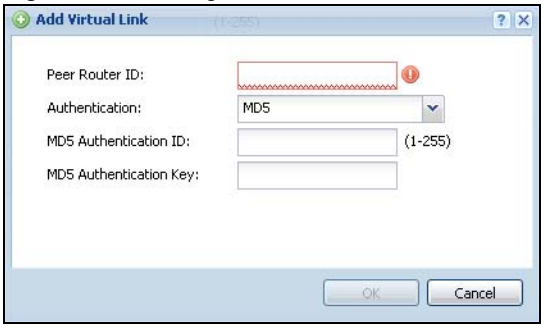
Table 76 Configuration > Network > Routing > OSPF > Add

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	Select the type of OSPF area. **Normal** - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. **Stub** - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. **NSSA** - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the **Type** is **Normal**. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
Add	Click this to create a new virtual link.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	This is the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	This is the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). Hover your cursor over this label to display the password. **MD5** uses an MD5 password and authentication ID (most secure). Hover your cursor over this label to display the authentication ID and key. **Same as Area** has the virtual link also use the **Authentication** settings above.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

10.3.3 Virtual Link Add/Edit Screen

The **Virtual Link Add/Edit** screen allows you to create a new virtual link or edit an existing one. When the OSPF add or edit screen (see Section 10.3.2 on page 206) has the Type set to Normal, a Virtual Link table displays. Click either the **Add** icon or an entry and the **Edit** icon to display a screen like the following.

Figure 120 Configuration > Network > Routing > OSPF > Add > Add



The following table describes the labels in this screen.

Table 77 Configuration > Network > Routing > OSPF > Add > Add

LABEL	DESCRIPTION
Peer Router ID	Enter the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure). **Same as Area** has the virtual link also use the **Authentication** settings above.
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

10.4 Routing Protocol Technical Reference

Here is more detailed information about RIP and OSPF.

Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated routing information. The transmitting and receiving routers must have the same key.

The ZyWALL supports three types of authentication for RIP and OSPF routing protocols:

- **None** - no authentication is used.
- **Text** – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- **MD5** – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The ZyWALL only accepts packets if these conditions are satisfied.

- The packet's authentication ID is the same as the authentication ID of the interface that received it.
- The packet's message-digest is the same as the one the ZyWALL calculates using the MD5 password.

For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the ZyWALL supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated **Authentication Type** field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

11

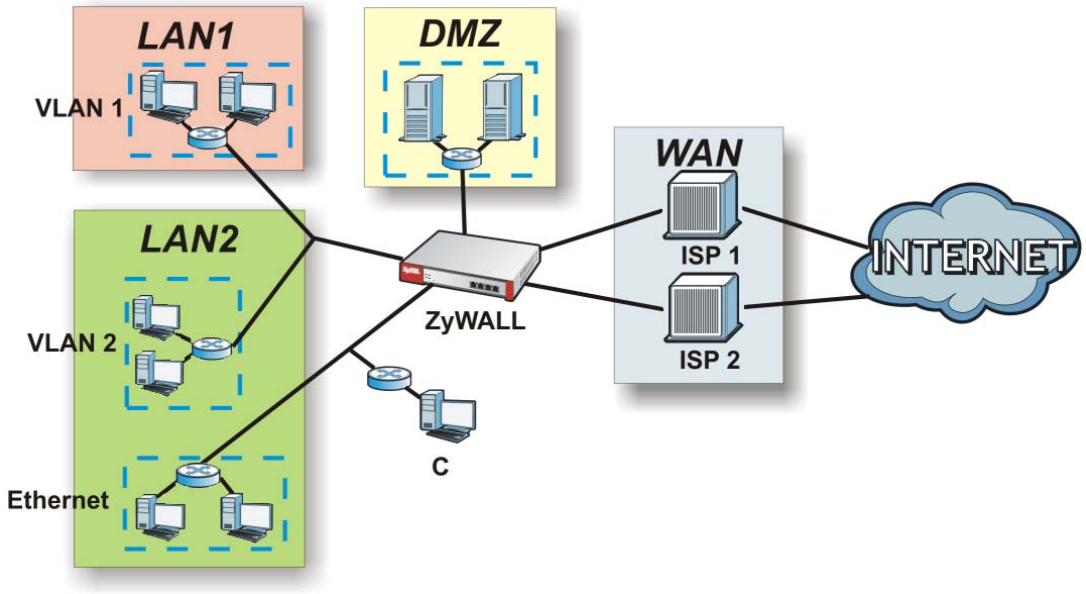
Zones

11.1 Zones Overview

Set up zones to configure network security and network policies in the ZyWALL. A zone is a group of interfaces and/or VPN tunnels. The ZyWALL uses zones instead of interfaces in many security and policy settings, such as firewall rules, Anti-X, and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 121 Example: Zones



11.1.1 What You Can Do in this Chapter

Use the **Zone** screens (see Section 11.2 on page 212) to manage the ZyWALL's zones.

11.1.2 What You Need to Know

Effects of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 121 on page 211, traffic between VLAN 2 and the Ethernet is intra-zone traffic.
- In each zone, you can either allow or prohibit all intra-zone traffic. For example, in Figure 121 on page 211, you might allow intra-zone traffic in the LAN zone but prohibit it in the WAN zone.
- You can set up firewall rules to control intra-zone traffic (for example, DMZ-to-DMZ), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 121 on page 211, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

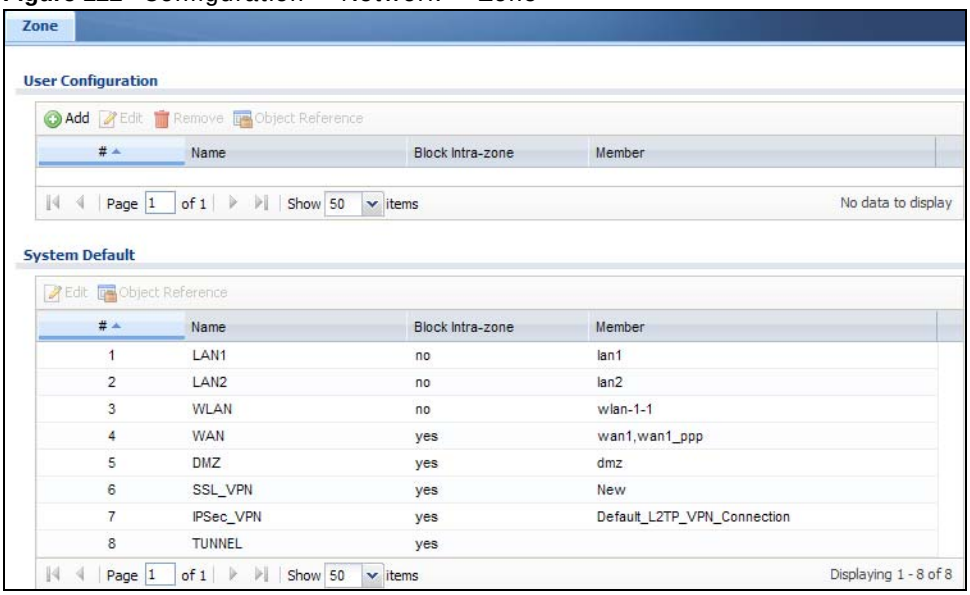
Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 121 on page 211, traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

11.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Configuration > Network > Zone**.

Figure 122 Configuration > Network > Zone



The following table describes the labels in this screen.

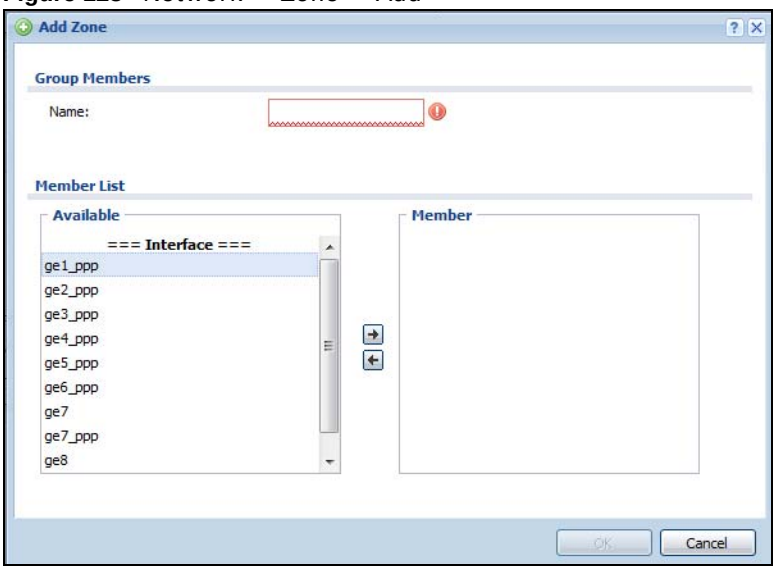
Table 78 Configuration > Network > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The ZyWALL comes with pre-configured **System Default** zones that you cannot delete. You can create your own **User Configuration** zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.

11.3 Zone Edit

The **Zone Edit** screen allows you to add or edit a zone. To access this screen, go to the **Zone** screen (see Section 11.2 on page 212), and click the **Add** icon or an **Edit** icon.

Figure 123 Network > Zone > Add



The following table describes the labels in this screen.

Table 79 Network > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	**Available** lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. **Member** lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

12

DDNS

12.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

12.1.1 What You Can Do in this Chapter

- Use the **DDNS** screen (see Section 12.2 on page 216) to view a list of the configured DDNS domain names and their details.
- Use the **DDNS Add/Edit** screen (see Section 12.2.1 on page 217) to add a domain name to the ZyWALL or to edit the configuration of an existing domain name.

12.1.2 What You Need to Know

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the ZyWALL. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ZyWALL supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 80 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Peanut Hull	Peanut Hull	www.oray.cn
3322	3322 Dynamic DNS, 3322 Static DNS	www.3322.org

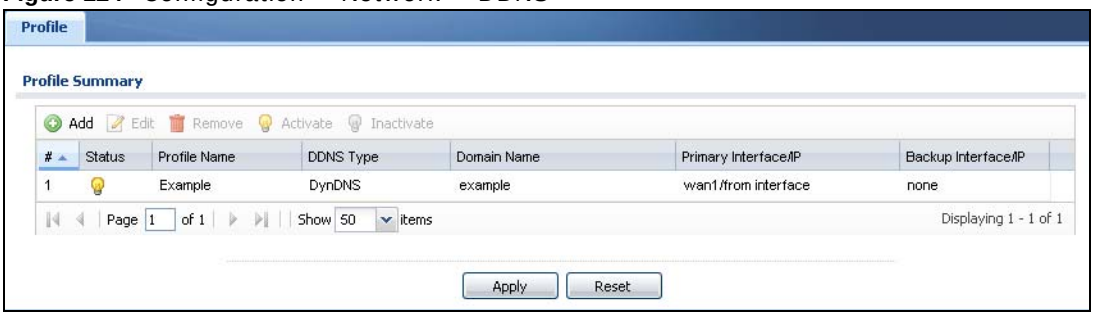
Note: Record your DDNS account's user name, password, and domain name to use to configure the ZyWALL.

After, you configure the ZyWALL, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

12.2 The DDNS Screen

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click **Configuration > Network > DDNS** to open the following screen.

Figure 124 Configuration > Network > DDNS



The following table describes the labels in this screen.

Table 81 Configuration > Network > DDNS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This is the number of an individual DDNS profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Type	This field displays which DDNS service you are using.
Domain Name	This field displays each domain name the ZyWALL can route.
Primary Interface/IP	This field displays the interface to use for updating the IP address mapped to the domain name followed by how the ZyWALL determines the IP address for the domain name. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. **custom** - The IP address is static.
Backup Interface/IP	This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the ZyWALL determines the IP address for the domain name. The ZyWALL uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. **custom** - The IP address is static.

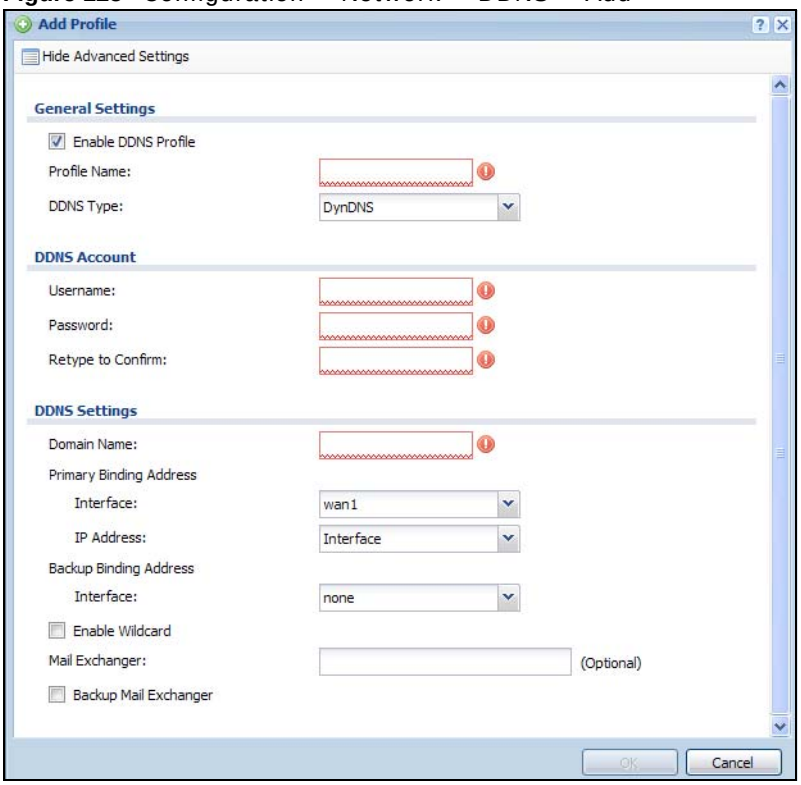
Table 81 Configuration > Network > DDNS (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

12.2.1 The Dynamic DNS Add/Edit Screen

The **DDNS Add / Edit** screen allows you to add a domain name to the ZyWALL or to edit the configuration of an existing domain name. Click **Configuration > Network > DDNS** and then an **Add** or **Edit** icon to open this screen.

Figure 125 Configuration > Network > DDNS > Add



The following table describes the labels in this screen.

Table 82 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this check box to use this DDNS entry.
Profile Name	When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the ZyWALL. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is read-only when you are editing an entry.
DDNS Type	Select the type of DDNS service you are using.

Table 82 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed. For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype to Confirm	Type the password again to confirm it.
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the ZyWALL determines the IP address that is mapped to your domain name in the DDNS server. The ZyWALL uses the **Backup Binding Address** if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface.
IP Address	The options available in this field vary by DDNS provider. **Interface** -The ZyWALL uses the IP address of the specified interface. This option appears when you select a specific interface in the **Primary Binding Address Interface** field. **Auto** - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server. Note: The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The ZyWALL still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary Binding Interface** settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface. Select **None** to not use a backup address.
IP Address	The options available in this field vary by DDNS provider. **Interface** -The ZyWALL uses the IP address of the specified interface. This option appears when you select a specific interface in the **Backup Binding Address Interface** field. **Auto** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server. Note: The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The ZyWALL still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.

Table 82 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Enable Wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.
Mail Exchanger	This option is only available with a DynDNS account. DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise leave the field blank. See www.dyndns.org for more information about mail exchangers.
Backup Mail Exchanger	This option is only available with a DynDNS account. Select this check box if you are using DynDNS's backup service for e-mail. With this service, DynDNS holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

13

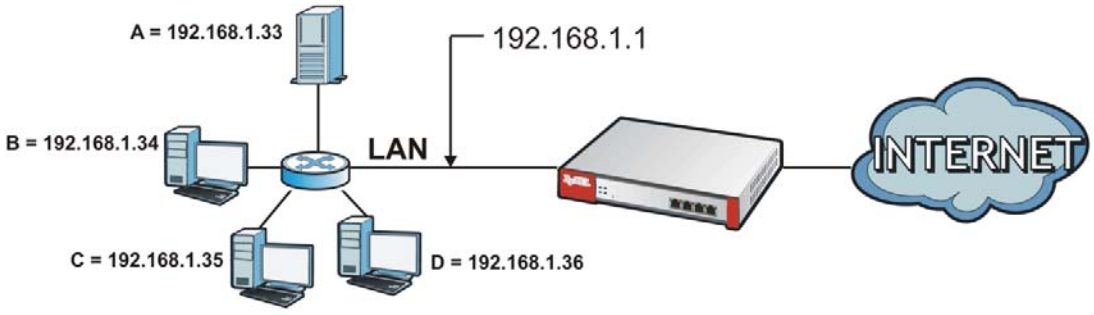
NAT

13.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network. Use Network Address Translation (NAT) to make computers on a private network behind the ZyWALL available outside the private network. If the ZyWALL has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 126 Multiple Servers Behind NAT Example



13.1.1 What You Can Do in this Chapter

Use the **NAT** screens (see Section 13.2 on page 222) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

13.1.2 What You Need to Know

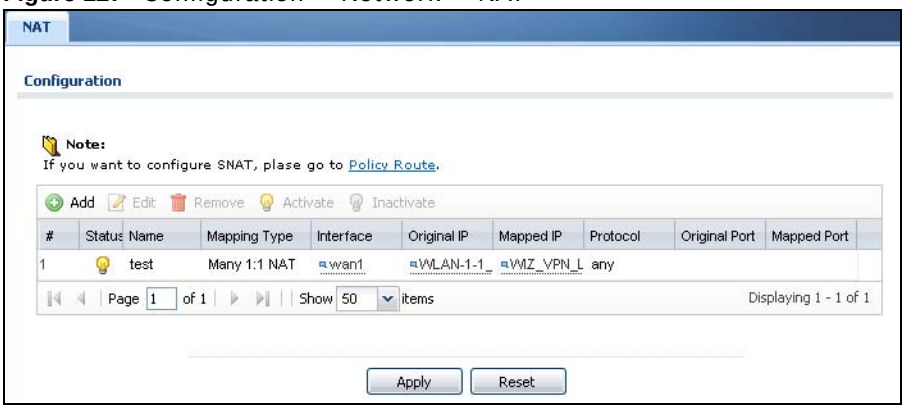
NAT is also known as virtual server, port forwarding, or port translation.

- See Section 13.3 on page 225 for technical background information related to these screens.

13.2 The NAT Screen

The **NAT** summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules. To access this screen, login to the Web Configurator and click **Configuration > Network > NAT**. The following screen appears, providing a summary of the existing NAT rules.

Figure 127 Configuration > Network > NAT



The following table describes the labels in this screen.

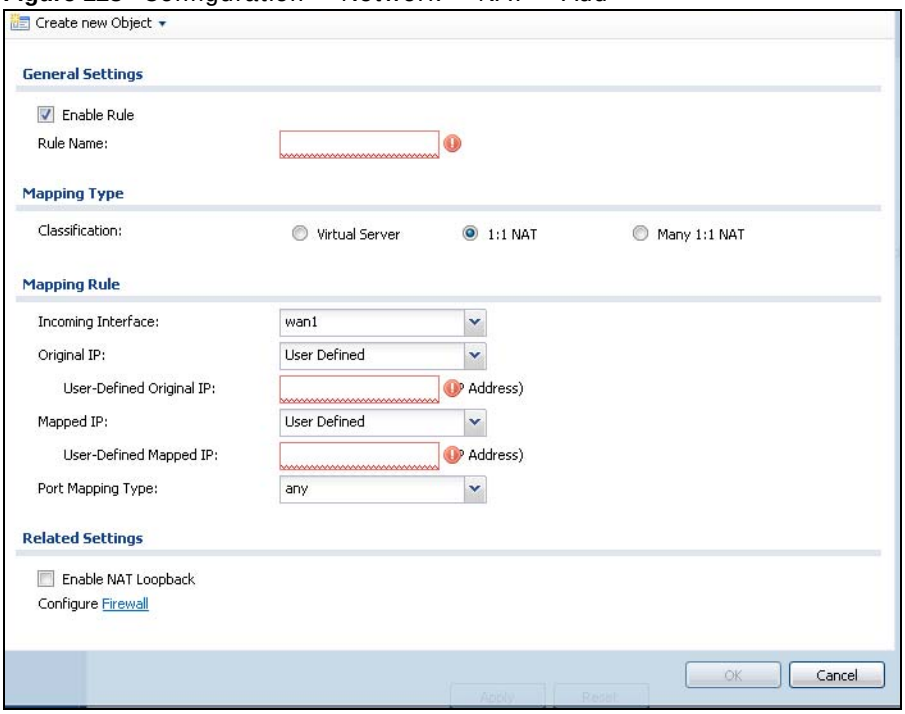
Table 83 Configuration > Network > NAT

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: **Virtual Server**, **1:1 NAT**, or **Many 1:1 NAT**.
Interface	This field displays the interface on which packets for the NAT entry are received.
Original IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays **any** if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this NAT entry. It displays **any** if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

13.2.1 The NAT Add/Edit Screen

The **NAT Add/Edit** screen lets you create new NAT rules and edit existing ones. To open this window, open the **NAT** summary screen. (See Section 13.2 on page 222.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 128 Configuration > Network > NAT > Add



The following table describes the labels in this screen.

Table 84 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Classification	Select what kind of NAT this rule is to perform. **Virtual Server** - This makes computers on a private network behind the ZyWALL available to a public network outside the ZyWALL (like the Internet). **1:1 NAT** - If the private network server will initiate sessions to the outside clients, select this to have the ZyWALL translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. **Many 1:1 NAT -** If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the ZyWALL translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses. One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.

Table 84 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.
Original IP	Specify the destination IP address of the packets received by this NAT rule's specified incoming interface. **any** - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. **User Defined** - Select this to manually enter an IP address in the **User Defined** field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it. Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.
User Defined Original IP	This field is available if **Original IP** is **User Defined**. Type the destination IP address that this NAT rule supports.
Original IP Subnet/ Range	This field displays for Many 1:1 NAT. Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Mapped IP	Select to which translated destination IP address this NAT rule forwards packets. **User Defined** - this NAT rule supports a specific IP address, specified in the **User Defined** field. HOST address - the drop-down box lists all the HOST address objects in the ZyWALL. If you select one of them, this NAT rule supports the IP address specified by the address object.
User Defined Original IP	This field is available if **Mapped IP** is **User Defined**. Type the translated destination IP address that this NAT rule supports.
Mapped IP Subnet/ Range	This field displays for **Many 1:1 NAT**. Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Port Mapping Type	Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (**Original IP**). Choices are: **Any** - this NAT rule supports all the destination ports. **Port** - this NAT rule supports one destination port. **Ports** - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service.
Protocol Type	This field is available if **Mapping Type** is **Port** or **Ports**. Select the protocol (**TCP**, **UDP**, or **Any**) used by the service requesting the connection.
Original Port	This field is available if **Mapping Type** is **Port**. Enter the original destination port this NAT rule supports.
Mapped Port	This field is available if **Mapping Type** is **Port**. Enter the translated destination port if this NAT rule forwards the packet.
Original Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of original destination ports this NAT rule supports.
Original End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of original destination ports this NAT rule supports.
Mapped Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.

Table 84 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Mapped End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	Enable NAT loopback to allow users connected to any interface (instead of just the specified **Incoming Interface**) to use the NAT rule's specified **Original IP** address to access the **Mapped IP** device. For users connected to the same interface as the **Mapped IP** device, the ZyWALL uses that interface's IP address as the source address for the traffic it sends from the users to the **Mapped IP** device. For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the ZyWALL uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 225 for more details. If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.
Firewall	By default the firewall blocks incoming connections from external addresses. After you configure your NAT rule settings, click the **Firewall** link to configure a firewall rule to allow the NAT rule's traffic to come in. The ZyWALL checks NAT rules before it applies To-ZyWALL firewall rules, so To-ZyWALL firewall rules do not apply to traffic that is forwarded by NAT rules. The ZyWALL still checks other firewall rules according to the source IP address and mapped IP address.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to return to the **NAT** summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

13.3 NAT Technical Reference

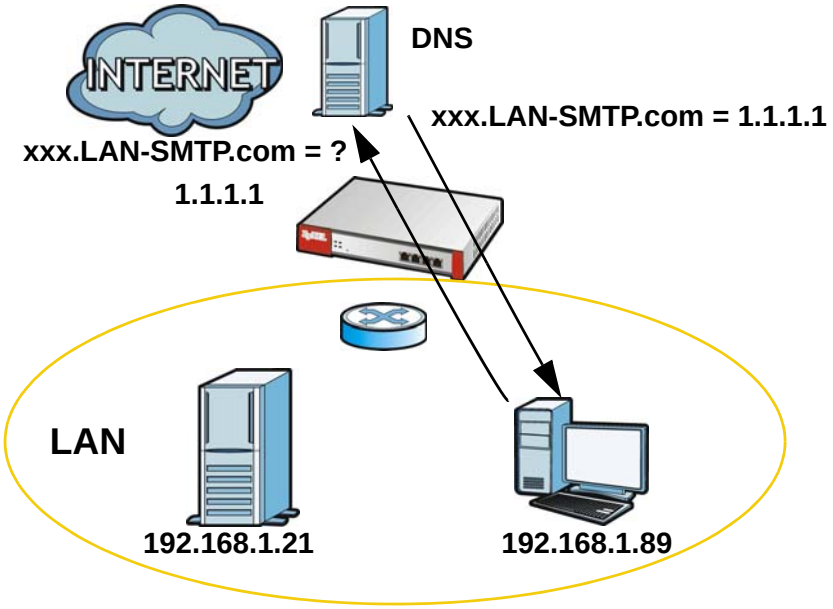
Here is more detailed information about NAT on the ZyWALL.

NAT Loopback

Suppose an NAT 1:1 rule maps a public IP address to the private IP address of a LAN SMTP e-mail server to give WAN users access. NAT loopback allows other users to also use the rule's original IP to access the mail server.

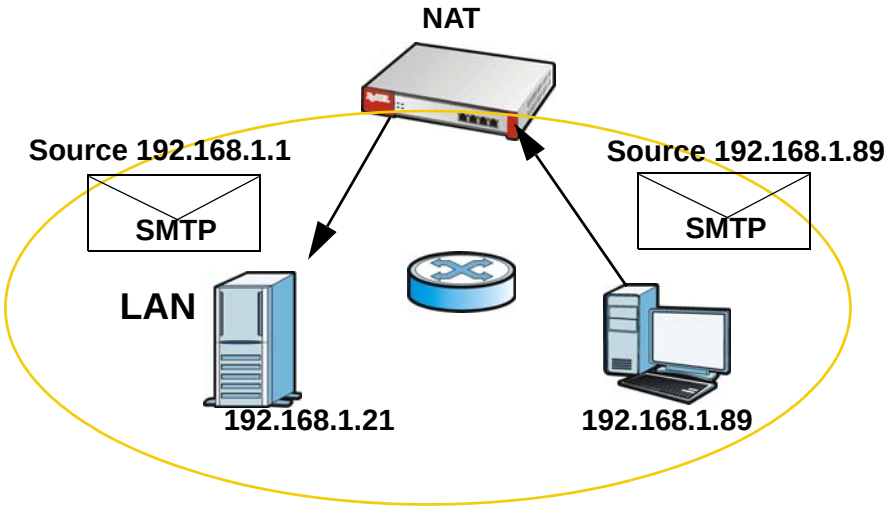
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 129 LAN Computer Queries a Public DNS Server



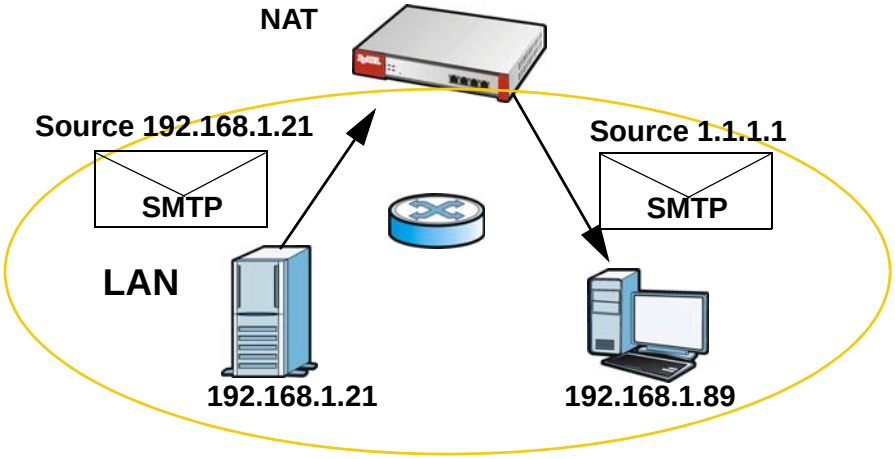
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the ZyWALL's LAN interface (192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 130 LAN to LAN Traffic



The LAN SMTP server replies to the ZyWALL's LAN IP address and the ZyWALL changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 131 LAN to LAN Return Traffic



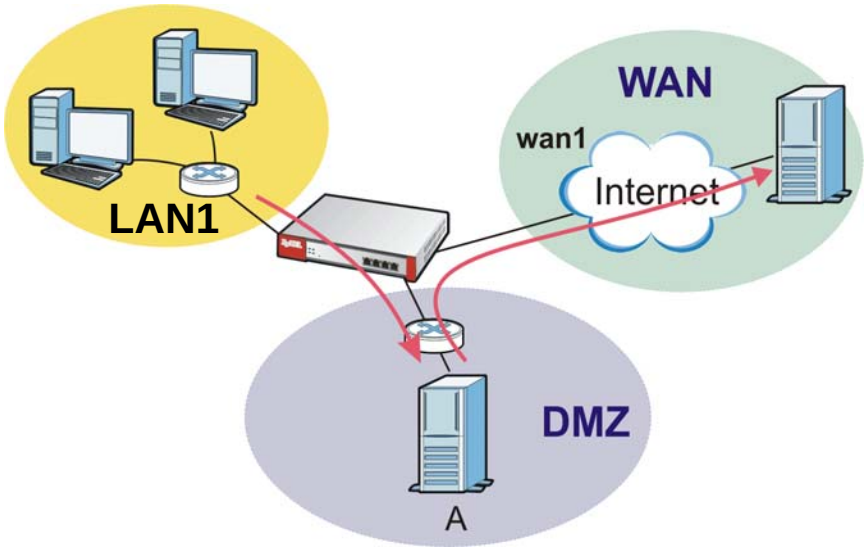
14

HTTP Redirect

14.1 Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL) to a web proxy server. In the following example, proxy server **A** is connected to the **DMZ** interface. When a client connected to the **LAN1** zone wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

Figure 132 HTTP Redirect Example



14.1.1 What You Can Do in this Chapter

Use the **HTTP Redirect** screens (see Section 14.2 on page 230) to display and edit the HTTP redirect rules.

14.1.2 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Firewall and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Firewall
2. HTTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the ZyWALL checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no firewall rule(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 132 on page 229 work, make sure you have the following settings.

For HTTP traffic between **lan1** and **dmz**:

- a from LAN1 to DMZ firewall rule (default) to allow HTTP requests from **lan1** to **dmz**. Responses to this request are allowed automatically.
- a HTTP redirect rule to forward HTTP traffic from **lan1** to proxy server **A**.

For HTTP traffic between **dmz** and **wan1**:

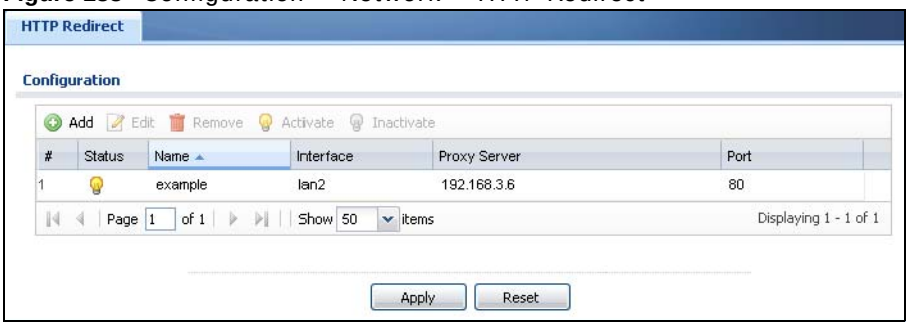
- a from DMZ to WAN firewall rule (default) to allow HTTP requests from **dmz** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

14.2 The HTTP Redirect Screen

To configure redirection of a HTTP request to a proxy server, click **Configuration > Network > HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.

Note: You can configure up to one HTTP redirect rule for each (incoming) interface.

Figure 133 Configuration > Network > HTTP Redirect



The following table describes the labels in this screen.

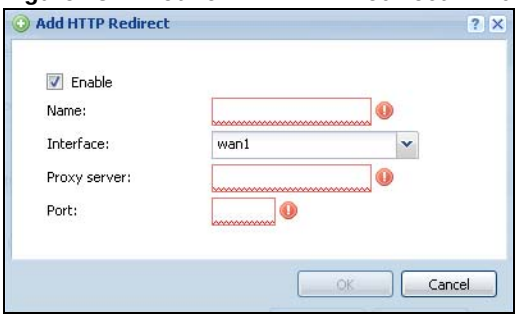
Table 85 Configuration > Network > HTTP Redirect

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the descriptive name of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

14.2.1 The HTTP Redirect Edit Screen

Click **Network > HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.

Figure 134 Network > HTTP Redirect > Edit



The following table describes the labels in this screen.

Table 86 Network > HTTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the HTTP redirect rule on or off.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which the HTTP request must be received for the ZyWALL to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

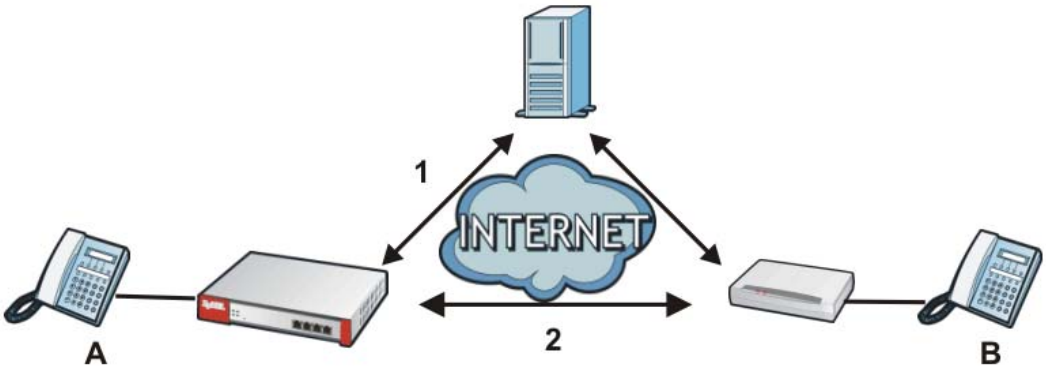
15.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the ZyWALL's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

Figure 135 SIP ALG Example



The ALG feature is only needed for traffic that goes through the ZyWALL's NAT.

15.1.1 What You Can Do in this Chapter

Use the **ALG** screen (Section 15.2 on page 236) to set up SIP, H.323, and FTP ALG settings.

15.1.2 What You Need to Know

Application Layer Gateway (ALG), NAT and Firewall

The ZyWALL can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL's NAT and firewall. The ZyWALL dynamically creates an implicit NAT session and firewall session for the application's traffic from the WAN to the LAN. The ALG on the ZyWALL supports all of the ZyWALL's NAT mapping types.

FTP ALG

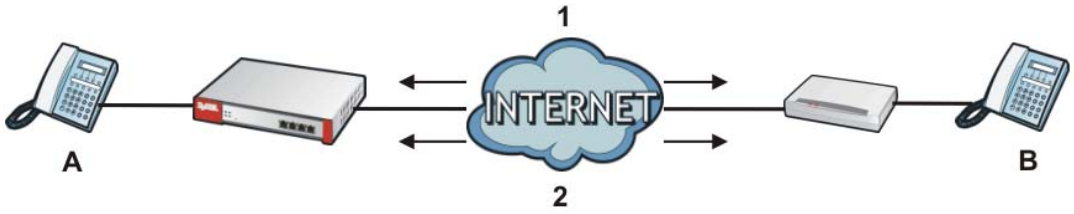
The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and firewall rules if you want to allow access to the server from the WAN.

H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- The ZyWALL allows H.323 audio connections.
- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 136 H.323 ALG Example



SIP ALG

- SIP phones can be in any zone (including LAN, DMZ, WAN), and the SIP server and SIP clients can be in the same network or different networks.
- There should be only one SIP server (total) on the ZyWALL's private networks. Any other SIP servers must be on the WAN. So for example you could have a Back-to-Back User Agent such as the IPPBX x6004 or an asterisk PBX on the DMZ or on the LAN but not on both.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the ZyWALL routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The firewall (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a specified port destination to pass through.
- The ZyWALL allows SIP audio connections.
- You do not need to use TURN (Traversal Using Relay NAT) for VoIP devices behind the ZyWALL when you enable the SIP ALG.

Peer-to-Peer Calls and the ZyWALL

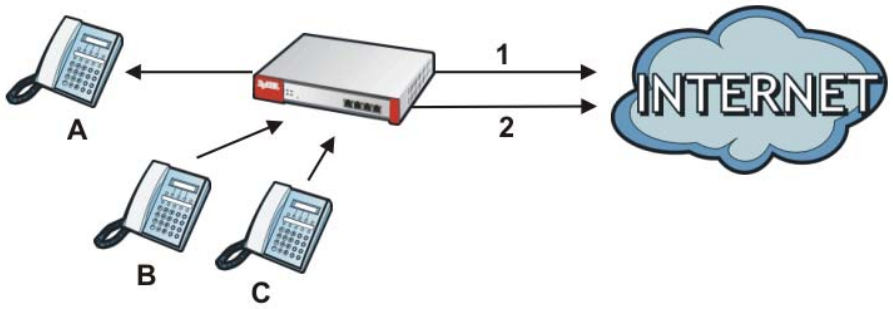
The ZyWALL ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the firewall and NAT (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the firewall and NAT (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the firewall and NAT to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 137 VoIP Calls from the WAN with Multiple Outgoing Calls

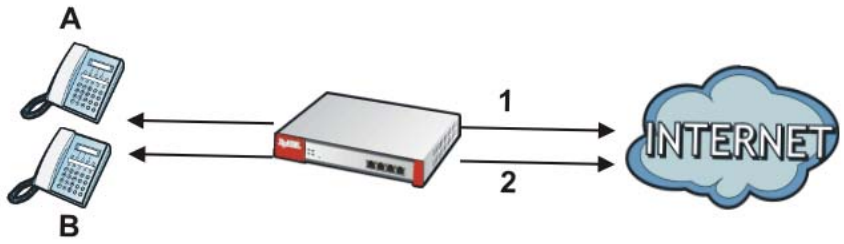


VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and NAT (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and NAT rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

Figure 138 VoIP with Multiple WAN IP Addresses



- See Section 15.3 on page 238 for ALG background/technical information.

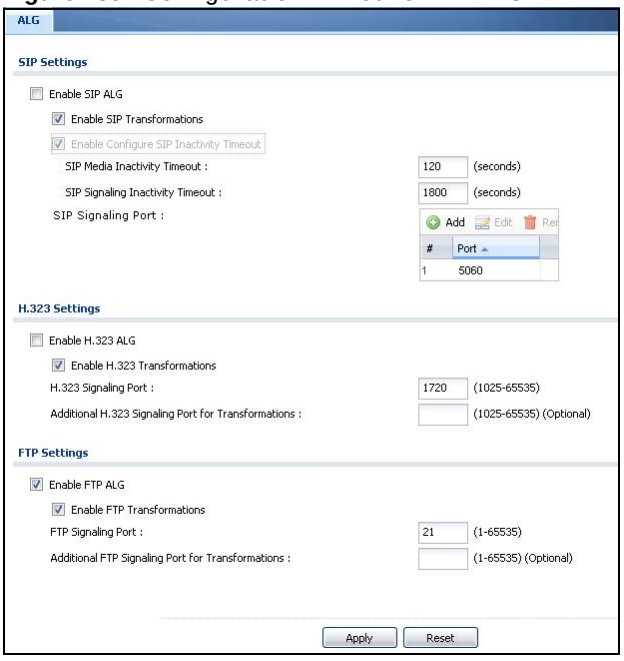
15.1.3 Before You Begin

You must also configure the firewall and enable NAT in the ZyWALL to allow sessions initiated from the WAN.

15.2 The ALG Screen

Click **Configuration > Network > ALG** to open the **ALG** screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Figure 139 Configuration > Network > ALG



The following table describes the labels in this screen.

Table 87 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the ZyWALL's NAT.
Enable SIP Transformations	Select this to have the ZyWALL modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.
Enable Configure SIP Inactivity Timeout	Select this option to have the ZyWALL apply SIP media and signaling inactivity time out limits.
SIP Media Inactivity Timeout	Use this field to set how many seconds (1~86400) the ZyWALL will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the ZyWALL deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling Inactivity Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL. If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout, the ZyWALL deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
Enable H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the ZyWALL's NAT.
Enable H.323 Transformations	Select this to have the ZyWALL modify IP addresses and port numbers embedded in the H.323 data payload. You do not need to use this if you have a H.323 device or server that will modify IP addresses and port numbers embedded in the H.323 data payload.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling Port for Transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the ZyWALL's NAT.
Enable FTP Transformations	Select this option to have the ZyWALL modify IP addresses and port numbers embedded in the FTP data payload to match the ZyWALL's NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the ZyWALL's NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

15.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

ALG

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has VoIP pass through enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The ZyWALL does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

16

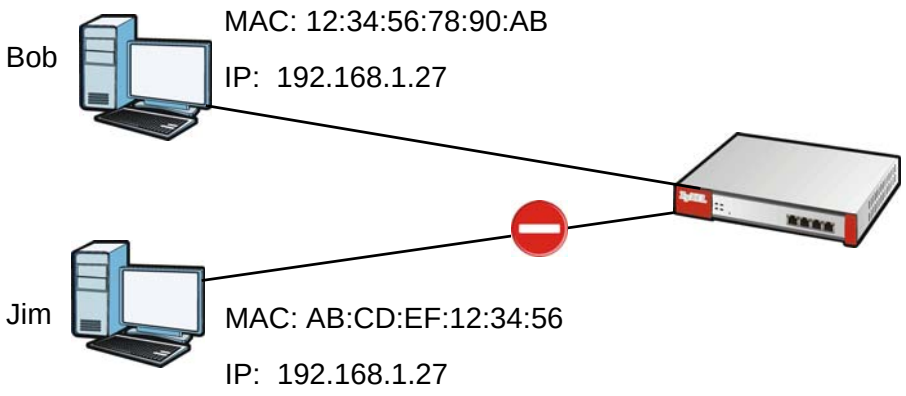
IP/MAC Binding

16.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The ZyWALL uses DHCP to assign IP addresses and records the MAC address it assigned to each IP address. The ZyWALL then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the ZyWALL.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 140 IP/MAC Binding Example



16.1.1 What You Can Do in this Chapter

- Use the **Summary** and **Edit** screens (Section 16.2 on page 242) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen (Section 16.3 on page 244) to configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding.

16.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the ZyWALL's dynamic and static DHCP entries.

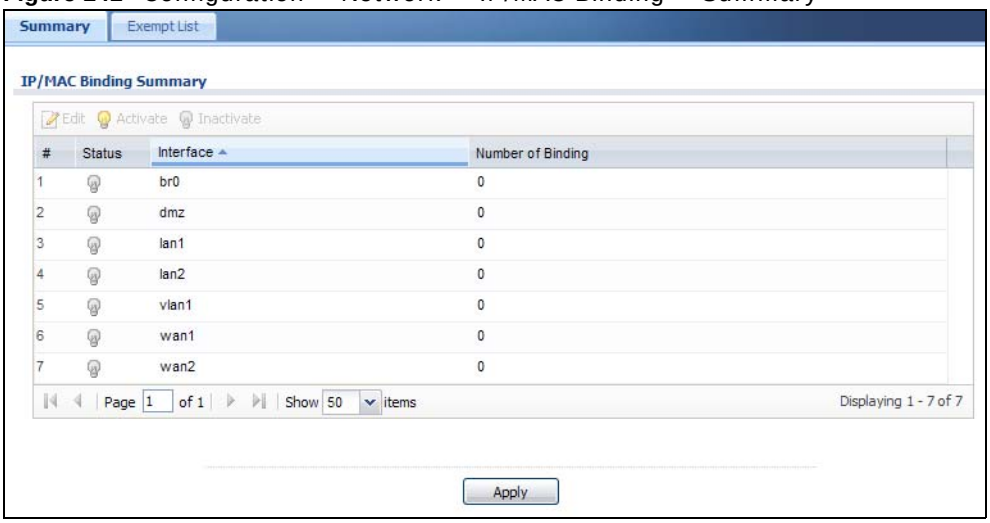
Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

16.2 IP/MAC Binding Summary

Click **Configuration > Network > IP/MAC Binding** to open the **IP/MAC Binding Summary** screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 141 Configuration > Network > IP/MAC Binding > Summary



The following table describes the labels in this screen.

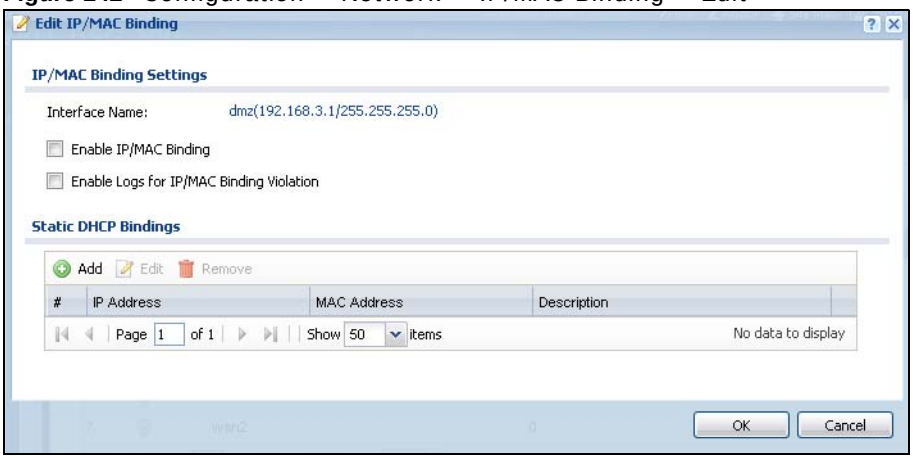
Table 88 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.
Apply	Click **Apply** to save your changes back to the ZyWALL.

16.2.1 IP/MAC Binding Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 142 Configuration > Network > IP/MAC Binding > Edit



The following table describes the labels in this screen.

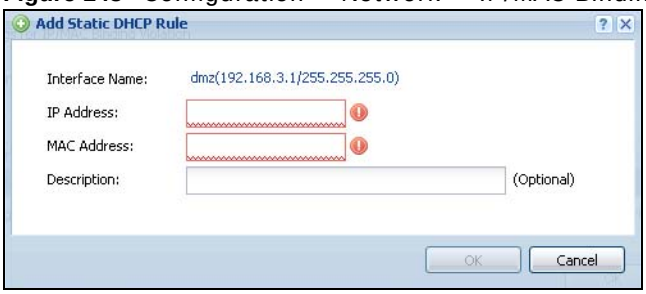
Table 89 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the ZyWALL and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address not assigned by the ZyWALL.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the ZyWALL assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the ZyWALL assigns the entry's IP address.
Description	This helps identify the entry.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

16.2.2 Static DHCP Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Click the **Add** or **Edit** icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 143 Configuration > Network > IP/MAC Binding > Edit > Add



The following table describes the labels in this screen.

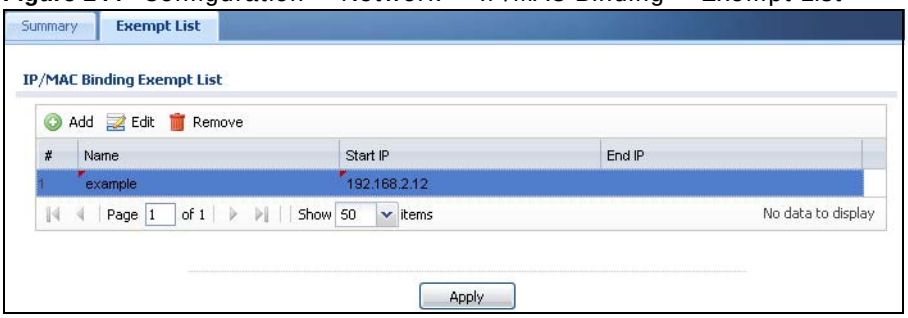
Table 90 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the ZyWALL and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the ZyWALL is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the ZyWALL assigns the entry's IP address.
Description	Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

16.3 IP/MAC Binding Exempt List

Click **Configuration > Network > IP/MAC Binding > Exempt List** to open the **IP/MAC Binding Exempt List** screen. Use this screen to configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding.

Figure 144 Configuration > Network > IP/MAC Binding > Exempt List



The following table describes the labels in this screen.

Table 91 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click **Edit** to modify the entry's settings.

Table 91 Configuration > Network > IP/MAC Binding > Exempt List (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the ZyWALL does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the ZyWALL does not apply IP/MAC binding.
Add icon	Click the **Add** icon to add a new entry. Click the **Remove** icon to delete an entry. A window displays asking you to confirm that you want to delete it.
Apply	Click **Apply** to save your changes back to the ZyWALL.

17

Inbound Load Balancing

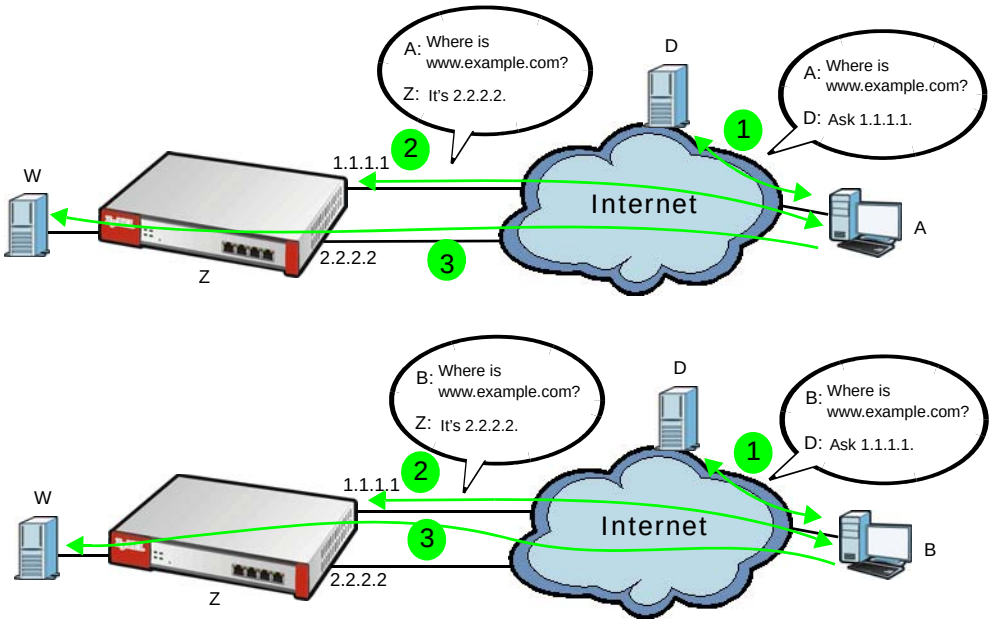
17.1 Inbound Load Balancing Overview

Inbound load balancing enables the ZyWALL to respond to a DNS query message with a different IP address for DNS name resolution. The ZyWALL checks which member interface has the least load and responds to the DNS query message with the interface's IP address.

In the following figure, an Internet host (**A**) sends a DNS query message to the DNS server (**D**) in order to resolve a domain name of www.example.com. DNS server **D** redirects it to the ZyWALL (**Z**)'s WAN1 with an IP address of 1.1.1.1. The ZyWALL receives the DNS query message and responds to it with the WAN2's IP address, 2.2.2.2, because the WAN2 has the least load at that moment.

Another Internet host (**B**) also sends a DNS query message to ask where www.example.com is. The ZyWALL responds to it with the WAN1's IP address, 1.1.1.1, since WAN1 has the least load this time.

Figure 145 DNS Load Balancing Example



17.1.1 What You Can Do in this Chapter

- Use the **Inbound LB** screen (see Section 17.2 on page 248) to view a list of the configured DNS load balancing rules.

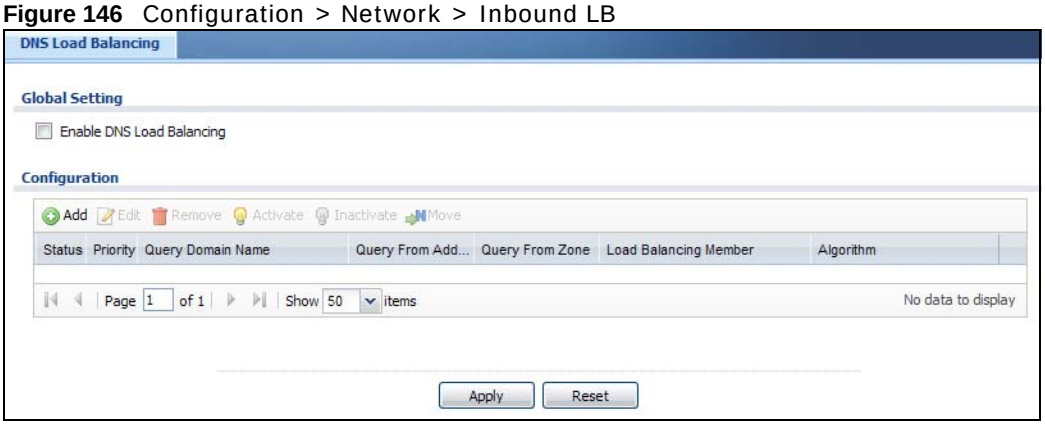
- Use the **Inbound LB Add/Edit** screen (see Section 17.2.1 on page 249) to add or edit a DNS load balancing rule.

17.2 The Inbound LB Screen

The **Inbound LB** screen provides a summary of all DNS load balancing rules and the details. You can also use this screen to add, edit, or remove the rules. Click **Configuration > Network > Inbound LB** to open the following screen.

Note: After you finish the inbound load balancing settings, go to firewall and NAT screens to configure the corresponding rule and virtual server to allow the Internet users to access your internal servers.

Figure 146 Configuration > Network > Inbound LB



The following table describes the labels in this screen.

Table 92 Configuration > Network > Inbound LB

LABEL	DESCRIPTION
Global Setting	
Enable DNS Load Balancing	Select this to enable DNS load balancing.
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This field displays the order in which the ZyWALL checks the member interfaces of this DNS load balancing rule.
Query Domain Name	This field displays the domain name for which the ZyWALL manages load balancing between the specified interfaces.

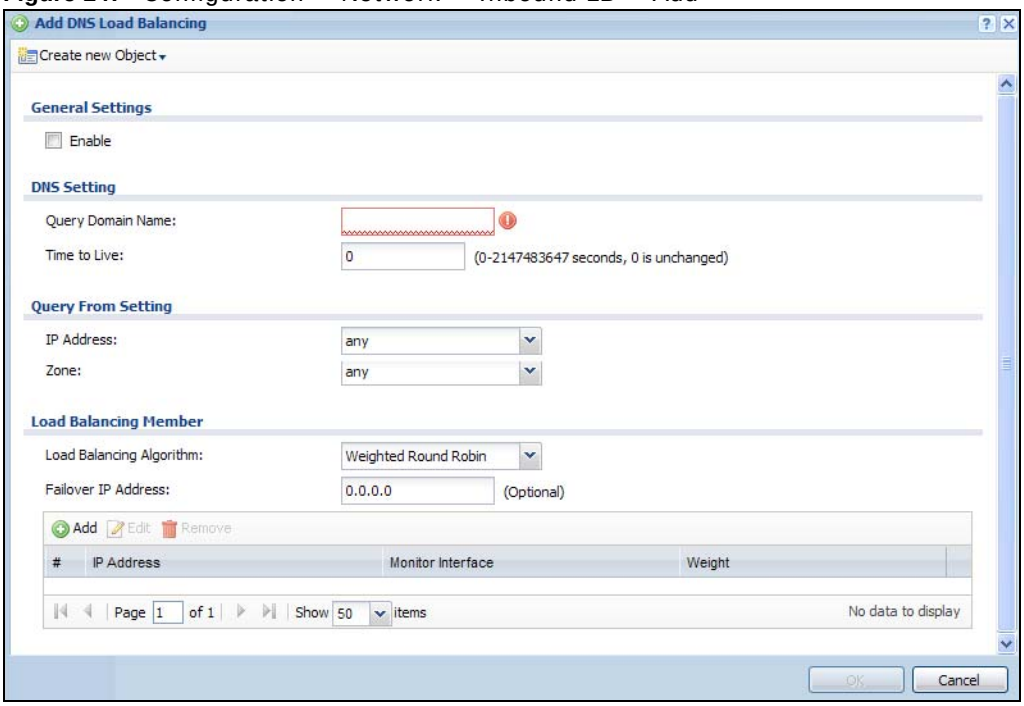
Table 92 Configuration > Network > Inbound LB (continued)

LABEL	DESCRIPTION
Query From Address	This field displays the source IP address of the DNS query messages to which the ZyWALL applies the DNS load balancing rule.
Query From Zone	The ZyWALL applies the DNS load balancing rule to the query messages received from this zone.
Load Balancing Member	This field displays the member interfaces which the ZyWALL manages for load balancing.
Algorithm	This field displays the load balancing method the ZyWALL uses for this DNS load balancing rule. **Weighted Round Robin** - Each member interface is assigned a weight. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the ZyWALL chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. **Least Connection** - The ZyWALL chooses choose a member interface which is handling the least number of sessions. **Least Load - Outbound** - The ZyWALL chooses a member interface which is handling the least amount of outgoing traffic. **Least Load - Inbound** - The ZyWALL chooses a member interface which is handling the least amount of incoming traffic. **Least Load - Total** - The ZyWALL chooses a member interface which is handling the least amount of outgoing and incoming traffic.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

17.2.1 The Inbound LB Add/Edit Screen

The **Add DNS Load Balancing** screen allows you to add a domain name for which the ZyWALL manages load balancing between the specified interfaces. You can configure the ZyWALL to apply DNS load balancing to some specific hosts only by configuring the **Query From** settings. Click **Configuration > Network > Inbound LB** and then the **Add** or **Edit** icon to open this screen.

Figure 147 Configuration > Network > Inbound LB > Add



The following table describes the labels in this screen.

Table 93 Configuration > Network > Inbound LB > Add/Edit

LABEL	DESCRIPTION
Create New Object	Use this to configure any new setting objects that you need to use in this screen.
General Settings	
Enable	Select this to enable this DNS load balancing rule.
DNS Setting	
Query Domain Name	Type up to 255 characters for a domain name for which you want the ZyWALL to manage DNS load balancing. You can use a wildcard (*) to let multiple domains match the name. For example, use *.example.com to specify any domain name that ends with “example.com” would match.
Time to Live	Enter the number of seconds the ZyWALL recommends DNS request hosts to keep the DNS entry in their caches before removing it. Enter 0 to have the ZyWALL not recommend this so the DNS request hosts will follow their DNS server’s TTL setting.
Query From Setting	
IP Address	Enter the IP address of a computer or a DNS server which makes the DNS queries upon which to apply this rule. DNS servers process client queries using recursion or iteration: • In recursion, DNS servers make recursive queries on behalf of clients. So you have to configure this field to the DNS server’s IP address when recursion is used. • In iteration, a client asks the DNS server and expects the best and immediate answer without the DNS server contacting other DNS servers. If the primary DNS server cannot provide the best answer, the client makes iteration queries to other configured DNS servers to resolve the name. You have to configure this field to the client’s IP address when iteration is used.
Zone	Select the zone of DNS query messages upon which to apply this rule.
Load Balancing Member	

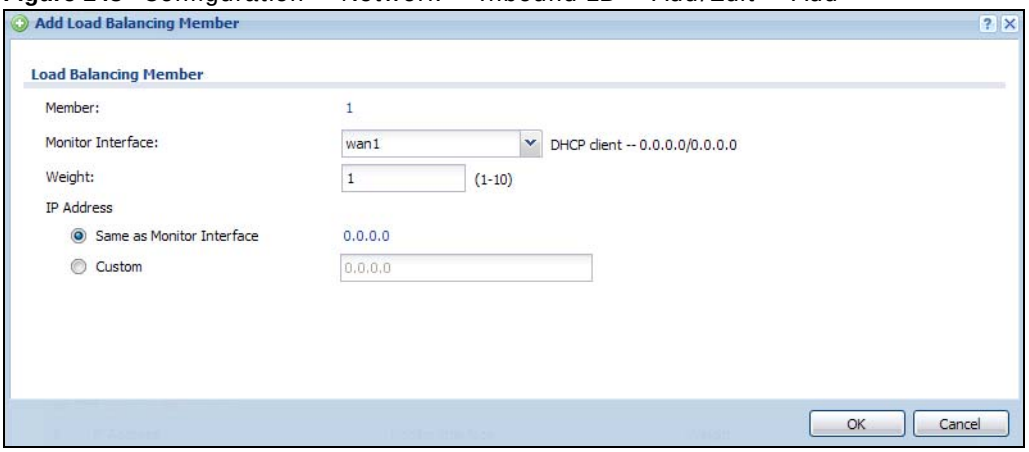
Table 93 Configuration > Network > Inbound LB > Add/Edit (continued)

LABEL	DESCRIPTION
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the ZyWALL chooses wan1 for 2 sessions' traffic and wan2 for every session's traffic in each round of 3 new sessions. Select **Least Connection** to have the ZyWALL choose the member interface which is handling the least number of sessions. Select **Least Load - Outbound** to have the ZyWALL choose the member interface which is handling the least amount of outgoing traffic. Select **Least Load - Inbound** to have the ZyWALL choose the member interface which is handling the least amount of incoming traffic. Select **Least Load - Total** to have the ZyWALL choose the member interface which is handling the least amount of outgoing and incoming traffic.
Failover IP Address	Enter an alternate IP address with which the ZyWALL will respond to a DNS query message when the load balancing algorithm cannot find any available interface.
Add	Click this to create a new member interface for this rule.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
#	This field displays the order in which the ZyWALL checks this rule's member interfaces.
IP Address	This field displays the IP address of the member interface.
Monitor Interface	This field displays the name of the member interface. The ZyWALL manages load balancing between the member interfaces.
Weight	This field is available if you selected **Weighted Round Robin** as the load balancing algorithm. This field displays the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

17.2.2 The Inbound LB Member Add/Edit Screen

The **Add Load Balancing Member** screen allows you to add a member interface for the DNS load balancing rule. Click **Configuration > Network > Inbound LB > Add or Edit** and then an **Add** or **Edit** icon to open this screen.

Figure 148 Configuration > Network > Inbound LB > Add/Edit > Add



The following table describes the labels in this screen.

Table 94 Configuration > Network > Inbound LB > Add/Edit > Add/Edit

LABEL	DESCRIPTION
Member	The ZyWALL checks each member interface's loading in the order displayed here.
Monitor Interface	Select an interface to associate it with the DNS load balancing rule. This field also displays whether the IP address is a static IP address (**Static**), dynamically assigned (**Dynamic**) or obtained from a DHCP server (**DHCP Client**), as well as the IP address and subnet mask.
Weight	This field is available if you selected **Weighted Round Robin** for the load balancing algorithm. Specify the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
IP Address	
Same as Monitor Interface	Select this to send the IP address displayed in the **Monitor Interface** field to the DNS query senders.
Custom	Select this and enter another IP address to send to the DNS query senders.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

18

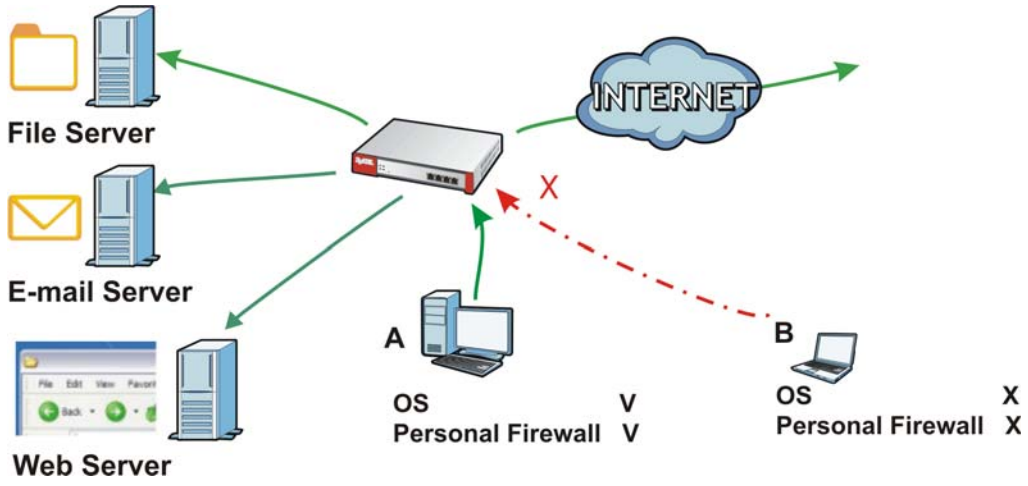
Authentication Policy

18.1 Overview

Use authentication policies to control who can access the network. After a user passes authentication the user's computer must meet the endpoint security object's Operating System (OS) option and security requirements to gain access.

In the following figure the ZyWALL's authentication policy requires endpoint security checking on local user **A**. **A** passes authentication and the endpoint security check and is given access. Local user **B** passes authentication but fails the endpoint security check and is denied access.

Figure 149 Authentication Policy Using Endpoint Security



18.1.1 What You Can Do in this Chapter

Use the **Configuration > Auth. Policy** screens (Section 18.2 on page 254) to create and manage authentication policies.

18.1.2 What You Need to Know

Authentication Policy and VPN

Authentication policies are applied based on a traffic flow's source and destination IP addresses. If VPN traffic matches an authentication policy's source and destination IP addresses, the user must pass authentication.

Multiple Endpoint Security Objects

You can set an authentication policy to use multiple endpoint security objects. This allows checking of computers with different OSs or security settings. When a client attempts to log in, the ZyWALL checks the client's computer against the endpoint security objects one-by-one. The client's computer must match one of the authentication policy's endpoint security objects in order to gain access.

Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the ZyWALL **Login** screen manually, you can configure the ZyWALL to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The ZyWALL does display the **Login** screen when users attempt to send other kinds of traffic.

The ZyWALL does not automatically route the request that prompted the login, however, so users have to make this request again.

Finding Out More

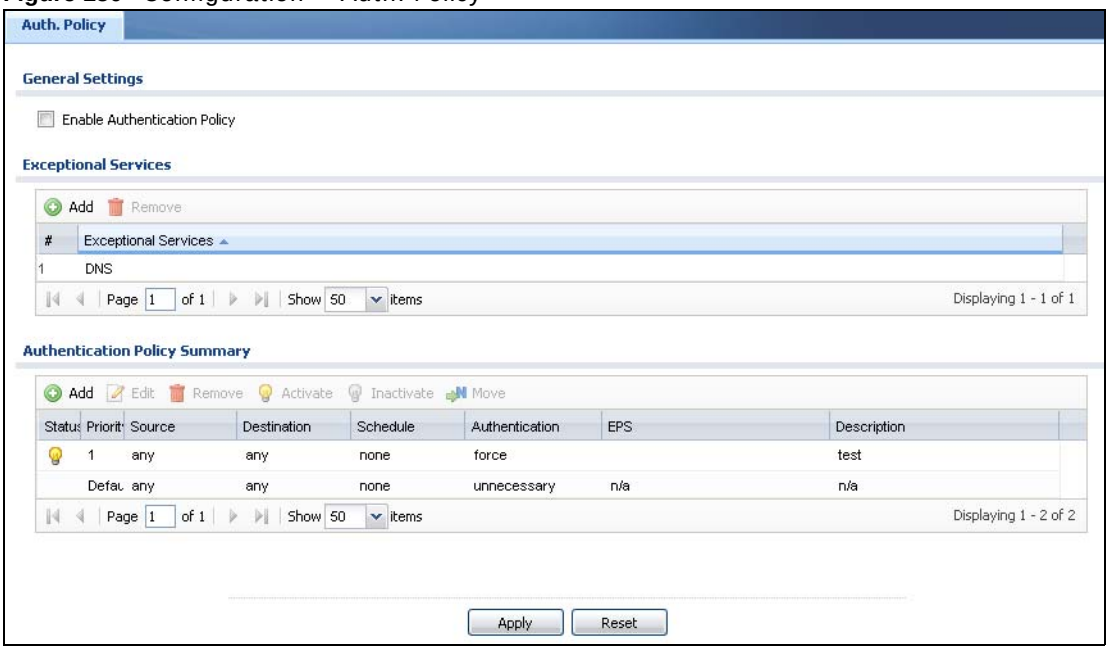
- See Section 18.3 on page 258 for an example of using an authentication policy for user-aware access control.

18.2 Authentication Policy Screen

The **Authentication Policy** screen displays the authentication policies you have configured on the ZyWALL.

Click **Configuration > Auth. Policy** to display the screen.

Figure 150 Configuration > Auth. Policy



The following table gives an overview of the objects you can configure.

Table 95 Configuration > Auth. Policy

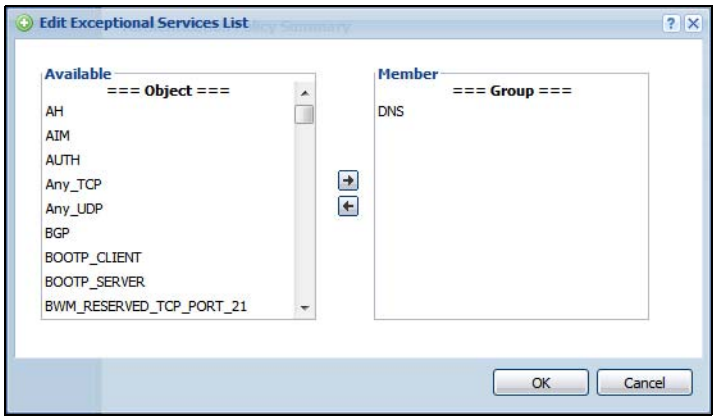
LABEL	DESCRIPTION
Enable Authentication Policy	Select this to turn on the authentication policy feature.
Exceptional Services	Use this table to list services that users can access without logging in. Click **Add** to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button to add them. The member services are the right. Select any service that you want to remove from the member list, and click the left arrow button to remove them. Keeping DNS as a member allows users' computers to resolve domain names into IP addresses. **Figure 151** Configuration > Auth. Policy > Add Exceptional Service  In the table, select one or more entries and click **Remove** to delete it or them.

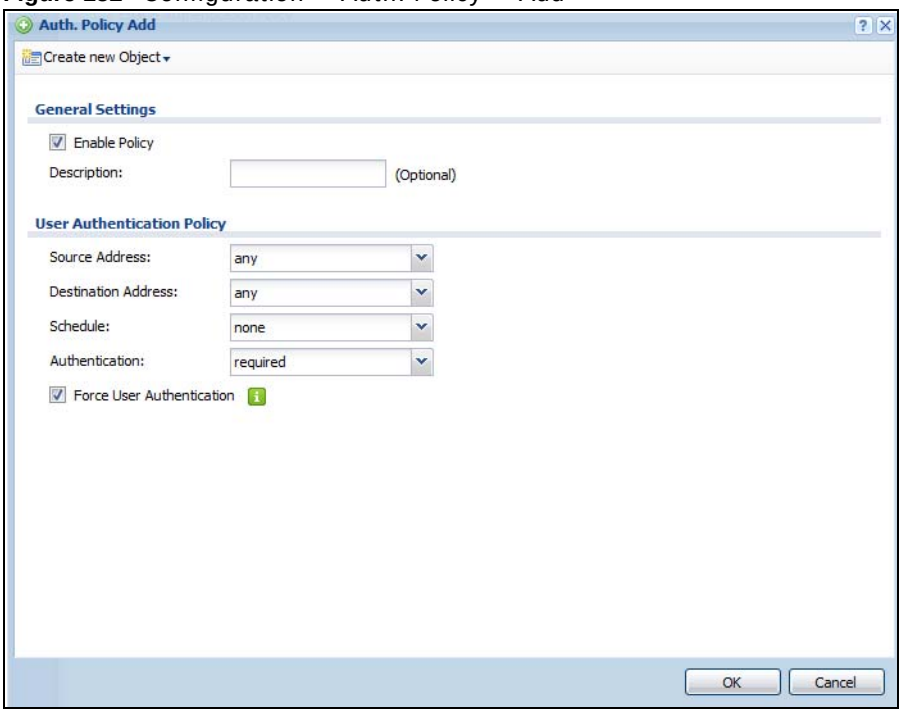
Table 95 Configuration > Auth. Policy (continued)

LABEL	DESCRIPTION
Authentication Policy Summary	Use this table to manage the ZyWALL's list of authentication policies.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. **Default** displays for the default authentication policy that the ZyWALL uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Source	This displays the source address object to which this policy applies.
Destination	This displays the destination address object to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. **none** means the policy is active at all times if enabled.
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. This is **n/a** for the default policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. They must manually go to the login screen. The ZyWALL will not redirect them to the login screen. **force** - Users need to be authenticated. The ZyWALL automatically displays the login screen whenever it routes HTTP traffic for users who have not logged in yet.
Description	If the entry has a description configured, it displays here.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

18.2.1 Creating/Editing an Authentication Policy

Click **Configuration > Auth. Policy** and then the **Add** (or **Edit**) icon to open the **Endpoint Security Edit** screen. Use this screen to configure an authentication policy.

Figure 152 Configuration > Auth. Policy > Add



The following table gives an overview of the objects you can configure.

Table 96 Configuration > Auth. Policy > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Policy	Select this check box to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the policy. Spaces are allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Source Address	Select a source address or address group for whom this policy applies. Select **any** if the policy is effective for every source. This is **any** and not configurable for the default policy.
Destination Address	Select a destination address or address group for whom this policy applies. Select **any** if the policy is effective for every destination. This is **any** and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select **none** and the rule is always effective. This is **none** and not configurable for the default policy.
Authentication	Select the authentication requirement for users when their traffic matches this policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. They must manually go to the login screen. The ZyWALL will not redirect them to the login screen.
Log	This field is available for the default policy. Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or not (**no**) for packets that match the default policy. See Chapter 38 on page 485 for more on logs.

Table 96 Configuration > Auth. Policy > Add (continued)

LABEL	DESCRIPTION
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the ZyWALL automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

18.3 User-aware Access Control Example

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the ZyWALL or by an external (AD, RADIUS, or LDAP) authentication server.

In this example the users are authenticated by an external RADIUS server at 192.168.1.200. First, set up the user accounts and user groups in the ZyWALL. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

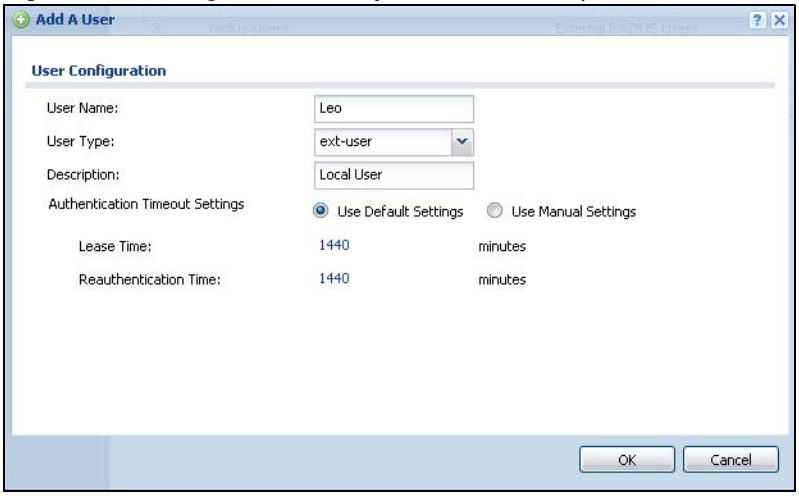
18.3.1 Set Up User Accounts

Set up user accounts in the RADIUS server. This example uses the Web Configurator. If you can export user names from the RADIUS server to a text file, then you might configure a script to create the user accounts instead.

1 Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **ext-user** because this user account is authenticated by an external server. Click **OK**.

Figure 153 Configuration > Object > User/Group > User > Add



3 Repeat this process to set up the remaining user accounts.

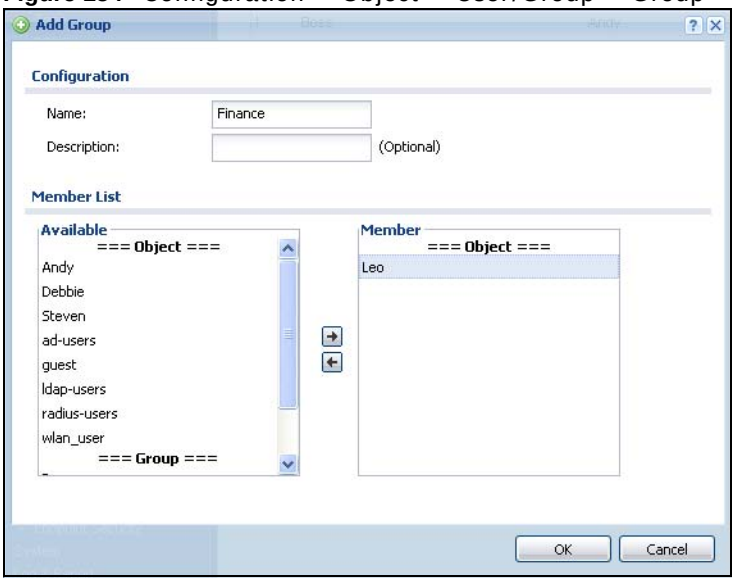
18.3.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

1 Click **Configuration > Object > User/Group > Group**. Click the **Add** icon.

2 Enter the name of the group. In this example, it is “Finance”. Then, select **User/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

Figure 154 Configuration > Object > User/Group > Group > Add



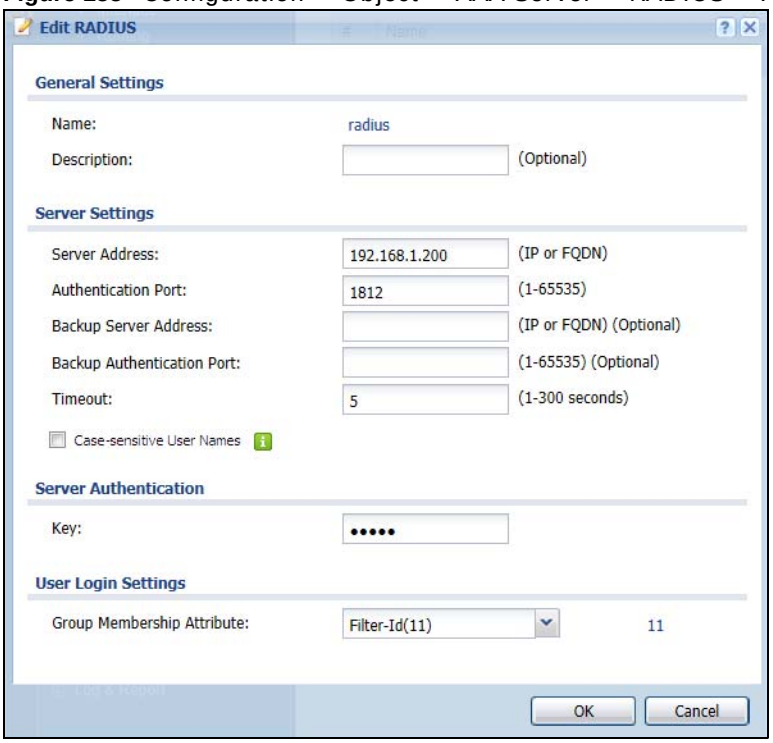
3 Repeat this process to set up the remaining user groups.

18.3.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the ZyWALL to use the authentication method. Finally, force users to log into the ZyWALL before it routes traffic for them.

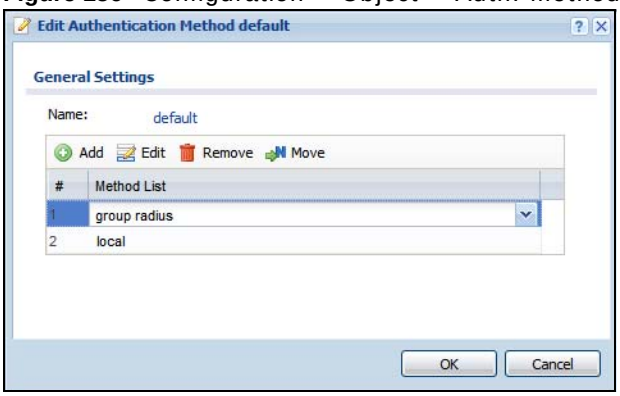
1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Configure the RADIUS server’s address, authentication port (1812 if you were not told otherwise), and key. Select **case-sensitive** if the RADIUS server checks user name casing. Click **Apply**.

Figure 155 Configuration > Object > AAA Server > RADIUS > Add



2 Click **Configuration > Object > Auth. Method**. Double-click the **default** entry. Click the **Add** icon. Select **group radius** because the ZyWALL should use the specified RADIUS server for authentication. Click **OK**.

Figure 156 Configuration > Object > Auth. method > Edit

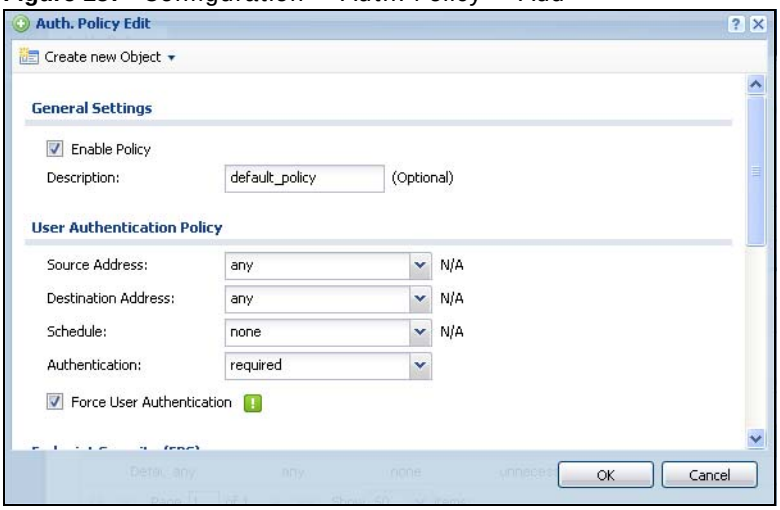


3 Click **Configuration > Auth. Policy**. In the **Authentication Policy Summary** section, click the **Add** icon.

4 Set up a default policy that forces every user to log into the ZyWALL before the ZyWALL routes traffic for them. Select **Enable**. Set the **Authentication** field to **required**, and make sure **Force User Authentication** is selected. Keep the rest of the default settings, and click **OK**.

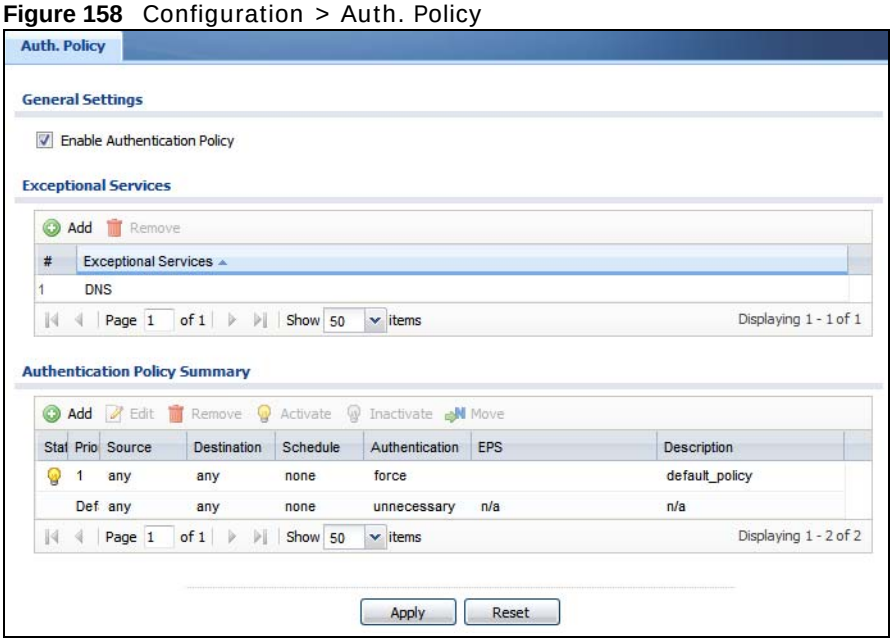
Note: The users must log in at the Web Configurator login screen before they can use HTTP or MSN.

Figure 157 Configuration > Auth. Policy > Add



In the **Auth. Policy** screen, select **Enable Authentication Policy** and click **Apply**.

Figure 158 Configuration > Auth. Policy



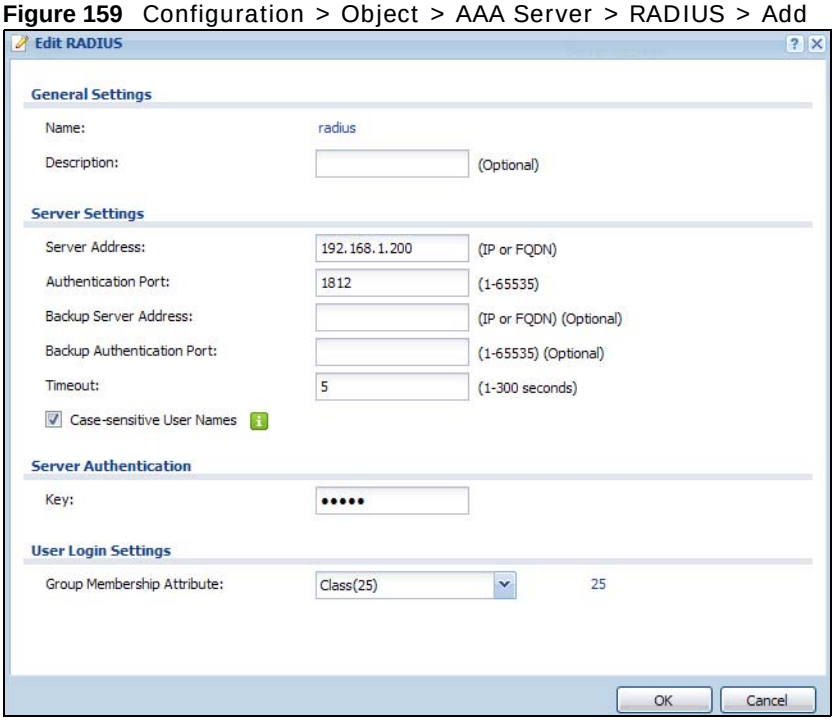
When the users try to browse the web (or use any HTTP/HTTPS application), the **Login** screen appears. They have to log in using the user name and password in the RADIUS server.

18.3.4 User Group Authentication Using the RADIUS Server

The previous example showed how to have a RADIUS server authenticate individual user accounts. If the RADIUS server has different user groups distinguished by the value of a specific attribute, you can make a couple of slight changes in the configuration to have the RADIUS server authenticate groups of user accounts defined in the RADIUS server.

1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Besides configuring the RADIUS server's address, authentication port, and key; set the **Group Membership Attribute** field to the attribute that the ZyWALL is to check to determine to which group a user belongs. This example uses **Class**. This attribute's value is called a group identifier; it determines to which group a user belongs. In this example the values are Finance, Engineer, Sales, and Boss. Select **case-sensitive** if the RADIUS server checks user name casing.

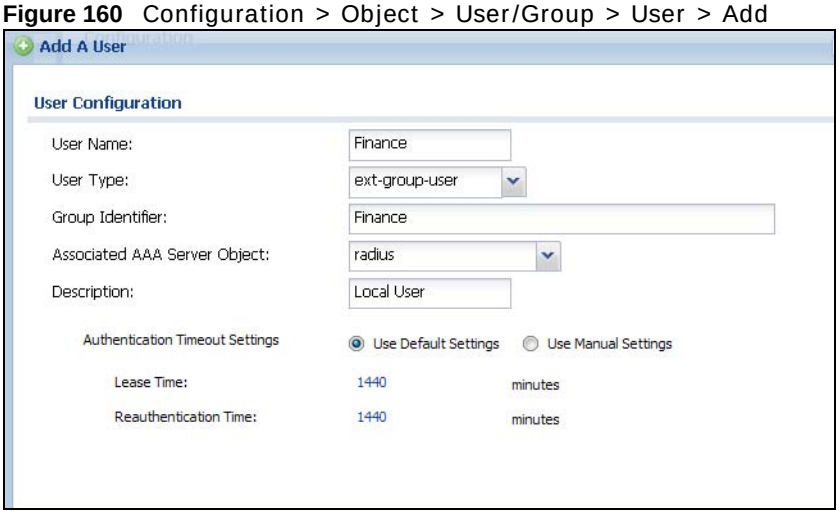
Figure 159 Configuration > Object > AAA Server > RADIUS > Add



2 Now you add ext-group-user user objects to identify groups based on the group identifier values. Set up one user account for each group of user accounts in the RADIUS server. Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

Enter a user name and set the **User Type** to **ext-group-user**. In the **Group Identifier** field, enter Finance, Engineer, Sales, or Boss and set the Associated AAA Server Object to radius.

Figure 160 Configuration > Object > User/Group > User > Add



3 Repeat this process to set up the remaining groups of user accounts.

19

Firewall

19.1 Overview

Use the firewall to block or allow services that use static port numbers. This example shows the ZyWALL's default firewall behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the firewall allows the response. However, the firewall blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone. The firewall allows VPN traffic between any of the networks.

Figure 161 Default Firewall Action



19.1.1 What You Can Do in this Chapter

- Use the **Firewall** screens (Section 19.2 on page 268) to enable or disable the firewall and asymmetrical routes, and manage and configure firewall rules.
- Use the **Session Limit** screens (see Section 19.3 on page 273) to limit the number of concurrent NAT/firewall sessions a client can use.

19.1.2 What You Need to Know

Stateful Inspection

The ZyWALL has a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces or VPN tunnels. Group the ZyWALL's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

Example Firewall Behavior

Firewall rules are grouped based on the direction of travel of packets to which they apply. Here is example firewall behavior for traffic going through the ZyWALL in various directions. See the **Configuration > Firewall** screen for default firewall behavior.

Note: At the time of writing the ZyWALL's VPN and GRE tunnels support IPv4 traffic so IPv6 firewall rules do not apply to IPSec, SSL VPN, and GRE tunnel traffic.

Table 97 Example Firewall Behavior

FROM ZONE TO ZONE	BEHAVIOR
From any to ZyWALL	DHCP traffic from any interface to the ZyWALL is allowed. DHCPv6 and Default_Allow_ICMPv6_Group traffic from any interface to the ZyWALL is allowed.
From LAN to any (other than the ZyWALL)	Traffic from the LAN to any of the networks connected to the ZyWALL is allowed.
From DMZ to WAN	Traffic from the DMZ to the WAN is allowed.
From IPSec VPN to any (other than the ZyWALL)	Traffic from the IPSec VPN zone to any of the networks connected to the ZyWALL is allowed.
From SSL VPN to any (other than the ZyWALL)	Traffic from the SSL VPN zone to any of the networks connected to the ZyWALL is allowed.
From TUNNEL to any (other than the ZyWALL)	Traffic from the TUNNEL zone to any of the networks connected to the ZyWALL is allowed.
From LAN to ZyWALL	Traffic from the LAN to the ZyWALL itself is allowed.
From DMZ to ZyWALL	DNS and NetBIOS traffic from the DMZ to the ZyWALL itself is allowed.
From WAN to ZyWALL	The default services listed in To-ZyWALL Rules on page 266 are allowed from the WAN to the ZyWALL itself. All other WAN to ZyWALL traffic is dropped.
From IPSec VPN to ZyWALL	Traffic from the IPSec VPN zone to the ZyWALL itself is allowed.
From SSL VPN to ZyWALL	Traffic from the SSL VPN zone to the ZyWALL itself is allowed.
From TUNNEL to ZyWALL	Traffic from the TUNNEL zone to the ZyWALL itself is allowed.
From any to any	Traffic that does not match any firewall rule is dropped. This includes traffic from the DMZ or WAN to any of the networks behind the ZyWALL and traffic other than DNS and NetBIOS from the DMZ to the ZyWALL. This also includes traffic to or from interfaces or VPN tunnels that are not assigned to a zone (extra-zone traffic).

To-ZyWALL Rules

Rules with **ZyWALL** as the **To Zone** apply to traffic going to the ZyWALL itself. By default:

- The firewall allows only LAN, WLAN, or WAN computers to access or manage the ZyWALL.
- The ZyWALL allows DHCP traffic from any interface to the ZyWALL.
- The ZyWALL allows DHCPv6 and Default_Allow_ICMPv6_Group traffic from any interface to the ZyWALL.
- The ZyWALL drops most packets from the DMZ zone to the ZyWALL itself and generates a log except for DNS and NetBIOS traffic.
- The ZyWALL drops most packets from the WLAN zone to the ZyWALL itself and generates a log except for BOOTP_SERVER, HTTP, HTTPS, and DNS traffic.
- The ZyWALL drops most packets from the WAN zone to the ZyWALL itself and generates a log except for AH, ESP, GRE, HTTPS, IKE, NATT (NATT applies to IPv4 only), and VRRP traffic.

When you configure a firewall rule for packets destined for the ZyWALL itself, make sure it does not conflict with your service control rule. See Chapter 37 on page 443 for more information about service control (remote management). The ZyWALL checks the firewall rules before the service control rules for traffic destined for the ZyWALL.

A **From Any To ZyWALL** direction rule applies to traffic from an interface which is not in a zone.

Global Firewall Rules

Firewall rules with **from any** and/or **to any** as the packet direction are called global firewall rules. The global firewall rules are the only firewall rules that apply to an interface or VPN tunnel that is not included in a zone. The **from any** rules apply to traffic coming from the interface and the **to any** rules apply to traffic going to the interface.

Firewall Rule Criteria

The ZyWALL checks the schedule, user name (user's login name on the ZyWALL), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

User Specific Firewall Rules

You can specify users or user groups in firewall rules. For example, to allow a specific user from any computer to access a zone by logging in to the ZyWALL, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL and will be disabled after the user logs out of the ZyWALL.

Firewall and VPN Traffic

After you create a VPN tunnel and add it to a zone, you can set the firewall rules applied to VPN traffic. If you add a VPN tunnel to an existing zone (the LAN1 zone for example), you can configure a new LAN1 to LAN1 firewall rule. If you add the VPN tunnel to a new zone (the VPN zone for example), you can configure rules for VPN traffic between the VPN zone and other zones or **From VPN To-ZyWALL** rules for VPN traffic destined for the ZyWALL.

Session Limits

Accessing the ZyWALL or network resources through the ZyWALL requires a NAT session and corresponding firewall session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the ZyWALL. The ZyWALL lets you limit the number of concurrent NAT/firewall sessions a client can use.

Finding Out More

- See Section 19.4 on page 276 for an example of creating firewall rules as part of configuring user-aware access control.

19.2 The Firewall Screen

Asymmetrical Routes

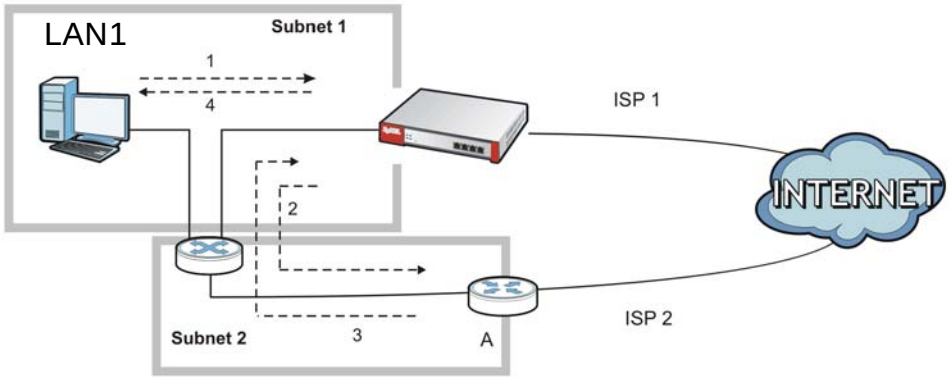
If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the ZyWALL to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyWALL reroutes the packet to gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the ZyWALL.
4. The ZyWALL then sends it to the computer on the LAN1 in **Subnet 1**.

Figure 162 Using Virtual Interfaces to Avoid Asymmetrical Routes

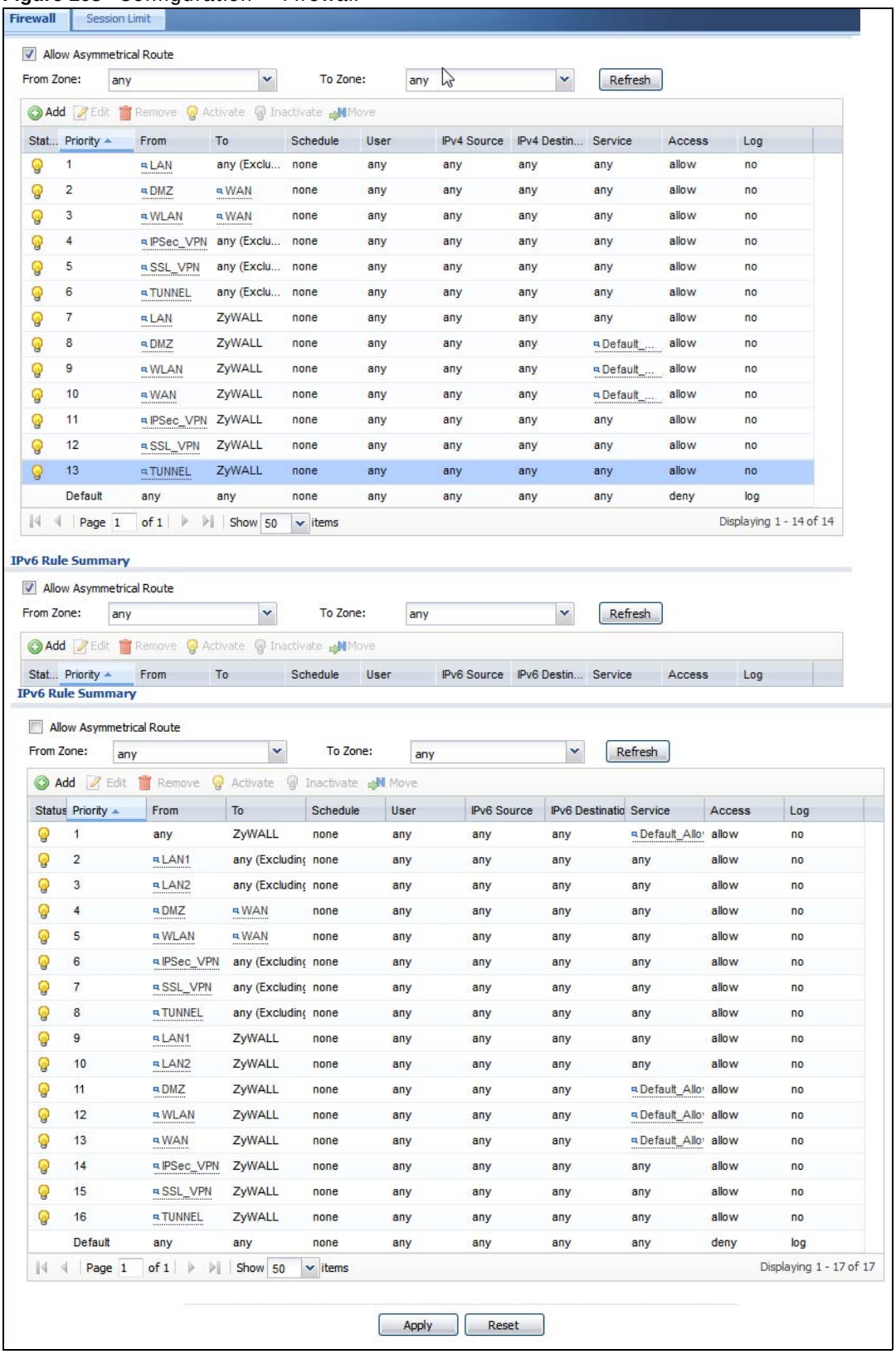


19.2.1 Configuring the Firewall Screen

Click **Configuration > Firewall** to open the **Firewall** screen. Use this screen to enable or disable the firewall and asymmetrical routes, set a maximum number of sessions per host, and display the configured firewall rules. Specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction. Note the following.

- Besides configuring the firewall, you also need to configure NAT rules to allow computers on the WAN to access LAN devices. See Chapter 13 on page 221 for more information.
- The ZyWALL applies NAT (Destination NAT) settings before applying the firewall rules. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding firewall rule to allow the traffic, you need to set the LAN IP address as the destination.
- The ordering of your rules is very important as rules are applied in sequence.

Figure 163 Configuration > Firewall


Firewall
Session Limit
Allow Asymmetrical Route
From Zone: any
To Zone: any
Refresh
Add Edit Remove Activate Inactivate Move
Stat... Priority From To Schedule User IPv4 Source IPv4 Destin... Service Access Log
1 LAN any (Exclu... none any any any any allow no
2 DMZ WAN none any any any any allow no
3 WLAN WAN none any any any any allow no
4 IPSec_VPN any (Exclu... none any any any any allow no
5 SSL_VPN any (Exclu... none any any any any allow no
6 TUNNEL any (Exclu... none any any any any allow no
7 LAN ZyWALL none any any any any allow no
8 DMZ ZyWALL none any any any Default_... allow no
9 WLAN ZyWALL none any any any Default_... allow no
10 WAN ZyWALL none any any any Default_... allow no
11 IPSec_VPN ZyWALL none any any any any allow no
12 SSL_VPN ZyWALL none any any any any allow no
13 TUNNEL ZyWALL none any any any any allow no
Default any any none any any any any deny log
Page 1 of 1 Show 50 items
Displaying 1 - 14 of 14
IPv6 Rule Summary
Allow Asymmetrical Route
From Zone: any
To Zone: any
Refresh
Add Edit Remove Activate Inactivate Move
Stat... Priority From To Schedule User IPv6 Source IPv6 Destin... Service Access Log
IPv6 Rule Summary
Allow Asymmetrical Route
From Zone: any
To Zone: any
Refresh
Add Edit Remove Activate Inactivate Move
Status Priority From To Schedule User IPv6 Source IPv6 Destinatio Service Access Log
1 any ZyWALL none any any any Default_Allo allow no
2 LAN1 any (Excludin none any any any any allow no
3 LAN2 any (Excludin none any any any any allow no
4 DMZ WAN none any any any any allow no
5 WLAN WAN none any any any any allow no
6 IPSec_VPN any (Excludin none any any any any allow no
7 SSL_VPN any (Excludin none any any any any allow no
8 TUNNEL any (Excludin none any any any any allow no
9 LAN1 ZyWALL none any any any any allow no
10 LAN2 ZyWALL none any any any any allow no
11 DMZ ZyWALL none any any any Default_Allo allow no
12 WLAN ZyWALL none any any any Default_Allo allow no
13 WAN ZyWALL none any any any Default_Allo allow no
14 IPSec_VPN ZyWALL none any any any any allow no
15 SSL_VPN ZyWALL none any any any any allow no
16 TUNNEL ZyWALL none any any any any allow no
Default any any none any any any any deny log
Page 1 of 1 Show 50 items
Displaying 1 - 17 of 17
Apply
Reset

The following table describes the labels in this screen.

Table 98 Configuration > Firewall

LABEL	DESCRIPTION
General Settings	
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control when the firewall is activated.
IPv4 / IPv6 Rule Summary	Separate firewall rules for IPv4 and IPv6 traffic appear when you enable the ZyWALL's global IPv6 option, otherwise the rules are just for IPv4 traffic.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets.
From Zone / To Zone	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, from **LAN1** to **LAN1** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN1. From **any** displays all the firewall rules for traffic going to the selected **To Zone**. To **any** displays all the firewall rules for traffic coming from the selected **From Zone**. From **any** to **any** displays all of the firewall rules. To **ZyWALL** rules are for traffic that is destined for the ZyWALL and control which computers can manage the ZyWALL.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.	
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence. **Default** displays for the default firewall behavior that the ZyWALL performs on traffic that does not match any other firewall rule.
From To	This is the direction of travel of packets to which the firewall rule applies.

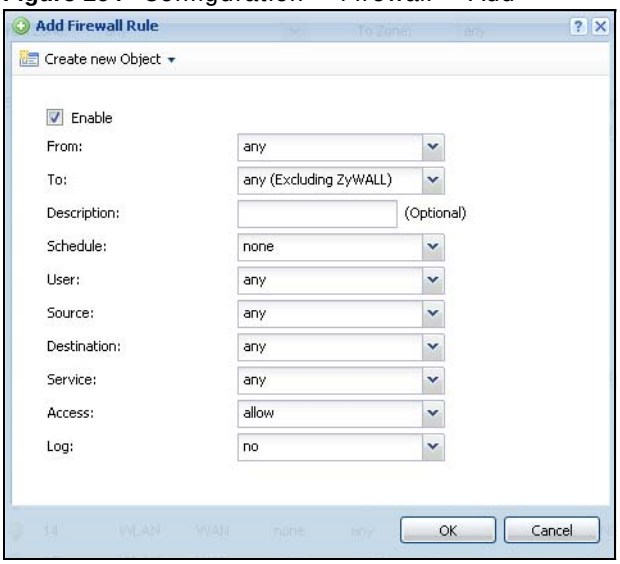
Table 98 Configuration > Firewall (continued)

LABEL	DESCRIPTION
Schedule	This field tells you the schedule object that the rule uses. **none** means the rule is active at all times if enabled.
User	This is the user name or user group name to which this firewall rule applies.
IPv4 / IPv6 Source	This displays the IPv4 or IPv6 source address object to which this firewall rule applies.
IPv4 / IPv6 Destination	This displays the IPv4 or IPv6 destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (**deny**), discards packets and sends a TCP reset packet to the sender (**reject**) or permits the passage of packets (**allow**).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

19.2.2 The Firewall Add/Edit Screen

In the **Firewall** screen, click the **Edit** or **Add** icon to display the **Firewall Rule Edit** screen.

Figure 164 Configuration > Firewall > Add



The following table describes the labels in this screen.

Table 99 Configuration > Firewall > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to activate the firewall rule.

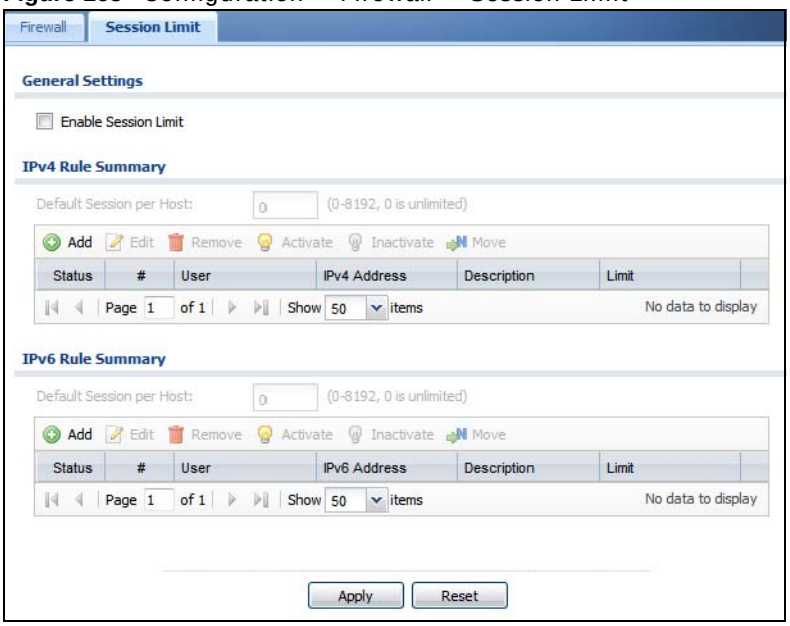
Table 99 Configuration > Firewall > Add (continued)

LABEL	DESCRIPTION
From To	For through-ZyWALL rules, select the direction of travel of packets to which the rule applies. **any** means all interfaces or VPN tunnels. **ZyWALL** means packets destined for the ZyWALL itself.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the firewall rule. Spaces are allowed.
Schedule	Select a schedule that defines when the rule applies. Otherwise, select **none** and the rule is always effective.
User	This field is not available when you are configuring a to-ZyWALL rule. Select a user name or user group to which to apply the rule. The firewall rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Source	Select an IPv4 address or address group to apply an IPv4 rule to traffic coming from it. Select an IPv6 address or address group to apply an IPv6 rule to traffic coming from it. Select **any** to apply an IPv4 rule to all traffic coming from IPv4 addresses. Select **any** to apply an IPv6 rule to all traffic coming from IPv6 addresses.
Destination	Select an IPv4 address or address group to apply an IPv4 rule to traffic going to it. Select an IPv6 address or address group to apply an IPv6 rule to traffic going to it. Select **any** to apply an IPv4 rule to all traffic going to IPv4 addresses. Select **any** to apply an IPv6 rule to all traffic going to IPv6 addresses.
Service	Select a service or service group from the drop-down list box.
Access	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **reject** to deny the packets and send a TCP reset packet to the sender. Any UDP packets are dropped without sending a response packet. Select **allow** to permit the passage of the packets.
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or not (**no**) when the rule is matched. See Chapter 38 on page 485 for more on logs.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

19.3 The Session Limit Screen

Click **Configuration > Firewall > Session Limit** to display the **Firewall Session Limit** screen. Use this screen to limit the number of concurrent NAT/firewall sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 165 Configuration > Firewall > Session Limit



The following table describes the labels in this screen.

Table 100 Configuration > Firewall > Session Limit

LABEL	DESCRIPTION
General Settings	
Enable Session limit	Select this check box to control the number of concurrent sessions hosts can have.
IPv4 / IPv6 Rule Summary	The IPv4 rules apply to IPv4 sessions. The IPv6 rules apply to IPv6 sessions.
Default Session per Host	Use this field to set a common limit to the number of concurrent NAT/firewall sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. Create rules below to apply other limits for specific users or addresses.
Rule Summary	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.

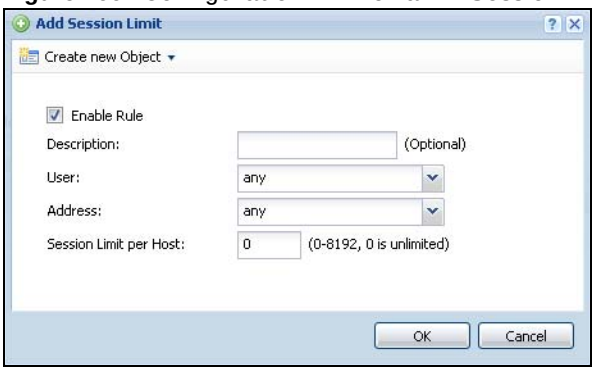
Table 100 Configuration > Firewall > Session Limit (continued)

LABEL	DESCRIPTION
User	This is the user name or user group name to which this session limit rule applies.
IPv4 Address	This is the IPv4 address object to which this session limit rule applies.
IPv6 Address	This is the IPv6 address object to which this session limit rule applies.
Description	This is the information configured to help you identify the rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

19.3.1 The Session Limit Add/Edit Screen

Click **Configuration > Firewall > Session Limit** and the **Add** or **Edit** icon to display the **Firewall Session Limit Edit** screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 166 Configuration > Firewall > Session Limit > Edit



The following table describes the labels in this screen.

Table 101 Configuration > Firewall > Session Limit > Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Select this check box to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select **any** and there is no need for user logging. Note: If you specified an IP address (or address group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Address	Select the IPv4 source address or address group to which this rule applies. Select **any** to apply the rule to all IPv4 source addresses.
IPv6 Address	Select the IPv6 source address or address group to which this rule applies. Select **any** to apply the rule to all IPv6 source addresses.

Table 101 Configuration > Firewall > Session Limit > Edit (continued)

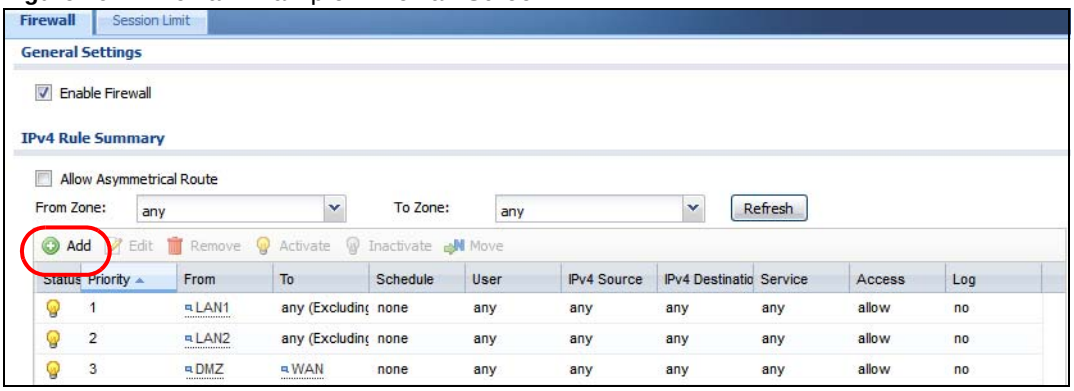
LABEL	DESCRIPTION
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/firewall sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **Firewall Session Limit** screen.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

19.4 Firewall Rule Configuration Example

The following Internet firewall rule example allows Doom players from the WAN to IP addresses 192.168.1.10 through 192.168.1.15 (Dest_1) on the LAN1.

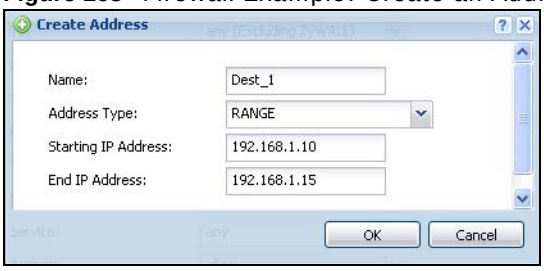
1 Click **Configuration > Firewall**. In the summary of IPv4 firewall rules click **Add** to configure a new first entry. The sequence (priority) of the rules is important since they are applied in order.

Figure 167 Firewall Example: Firewall Screen



2 At the top of the screen, click **Create new Object > Address** to configure an address object. Configure it as follows and click **OK**.

Figure 168 Firewall Example: Create an Address Object



3 Click **Create new Object > Service** to configure a service object for Doom (UDP port 666). Configure it as follows and click **OK**.

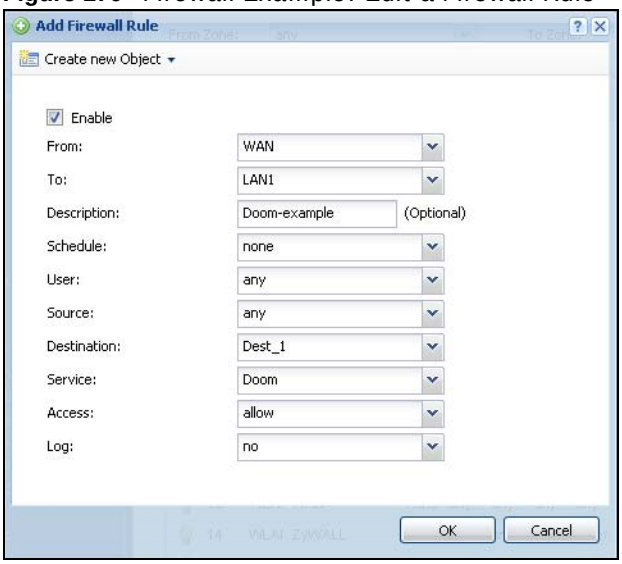
Figure 169 Firewall Example: Create a Service Object



4 Select **From WAN** and **To LAN1** and enter a name for the firewall rule.

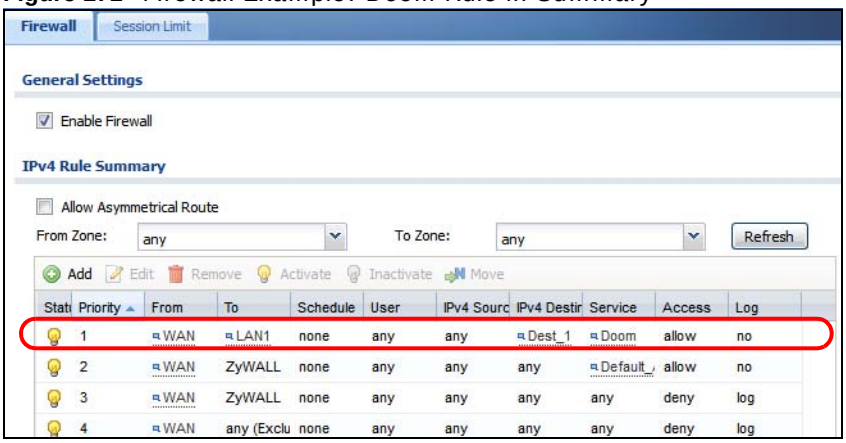
Select **Dest_1** for the **Destination** and **Doom** as the **Service**. Enter a description and configure the rest of the screen as follows. Click **OK** when you are done.

Figure 170 Firewall Example: Edit a Firewall Rule



5 The firewall rule appears in the firewall rule summary.

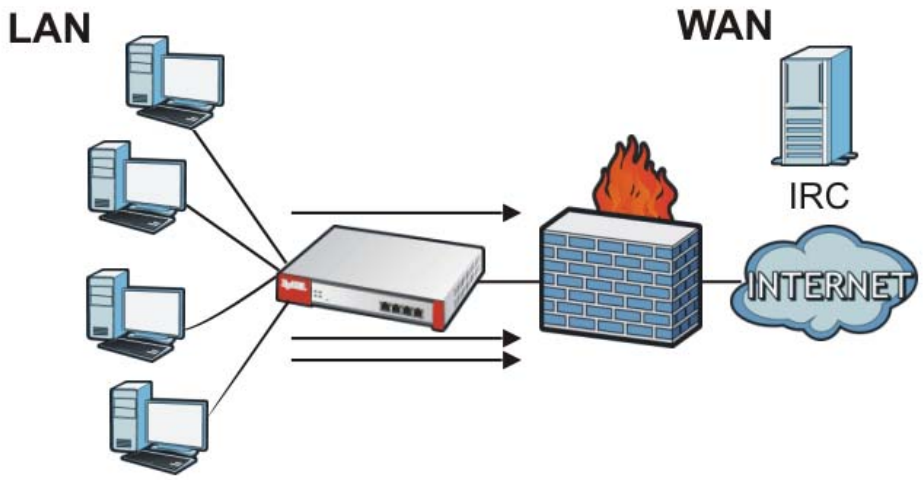
Figure 171 Firewall Example: Doom Rule in Summary



19.5 Firewall Rule Example Applications

Suppose you decide to block LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

Figure 172 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following rules.

Table 102 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all LAN1 to WAN traffic.

The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the second rule and the ZyWALL forwards it.

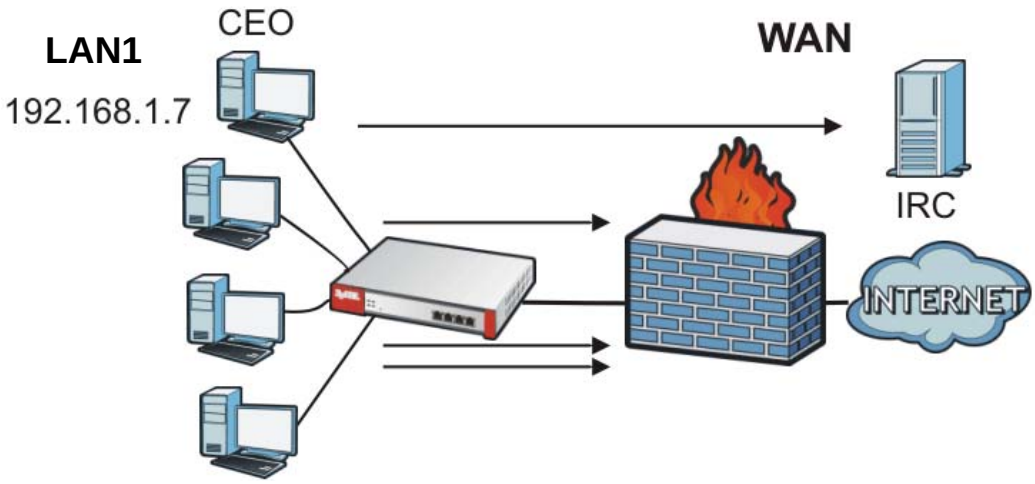
Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN rule that allows IRC traffic from any computer through which the CEO logs into the ZyWALL with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- Has a static IP address,

  or
- You configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see DHCP Settings on page 173 for information on DHCP).

Now you configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

Figure 173 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 103 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN rule with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your firewall would have the following configuration.

Table 104 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the ZyWALL with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN1 to WAN IRC traffic. If the rule that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

20

IPSec VPN

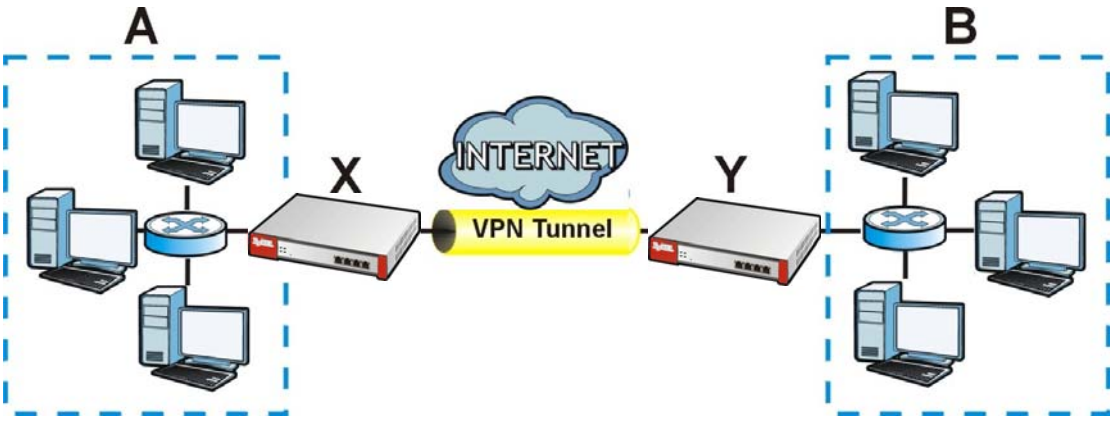
20.1 Virtual Private Networks (VPN) Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

IPSec VPN

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The ZyWALL can also combine multiple IPSec VPN connections into one secure network. Here local ZyWALL **X** uses an IPSec VPN tunnel to remote (peer) ZyWALL **Y** to connect the local (**A**) and remote (**B**) networks.

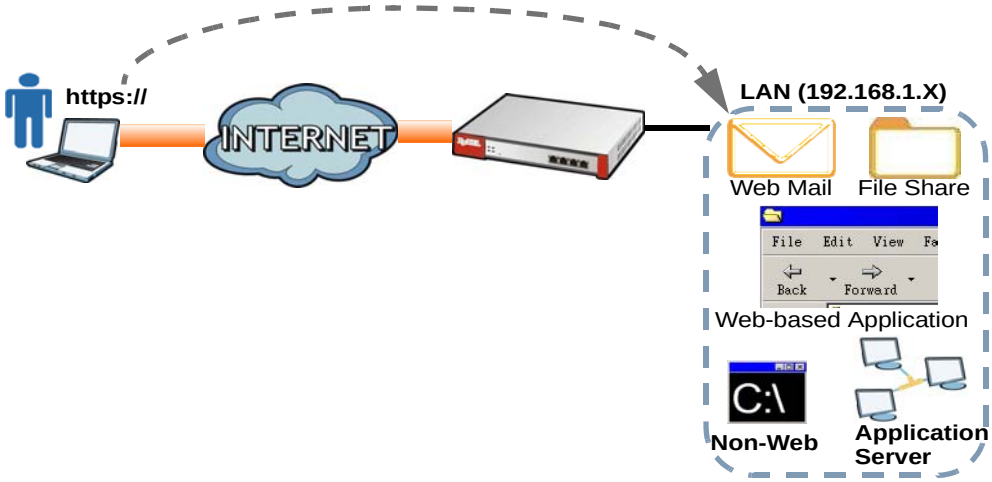
Figure 174 IPSec VPN Example



SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the ZyWALL's VPN solutions. A user just browses to the ZyWALL's web address and enters his user name and password to securely connect to the ZyWALL's network. Remote users do not need to configure security settings. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network. See Chapter 21 on page 317 for more on SSL VPN.

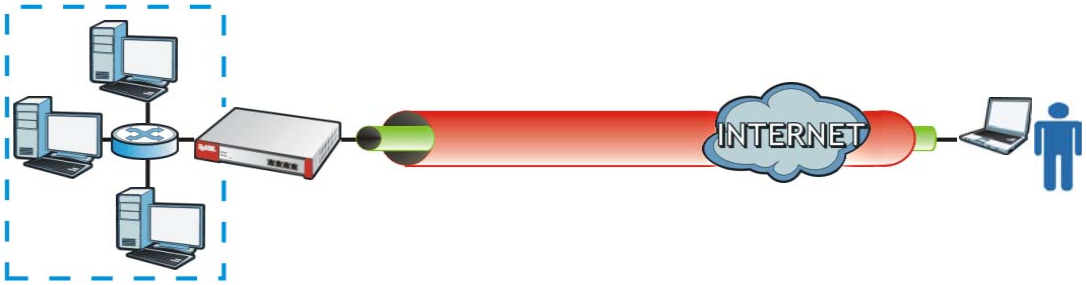
Figure 175 SSL VPN



L2TP VPN

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the ZyWALL. The remote users do not need their own IPSec gateways or third-party VPN client software. For example, configure sales representatives' laptops, tablets, or smartphones to securely connect to the ZyWALL's network. See Chapter 24 on page 345 for more on L2TP over IPSec.

Figure 176 L2TP VPN



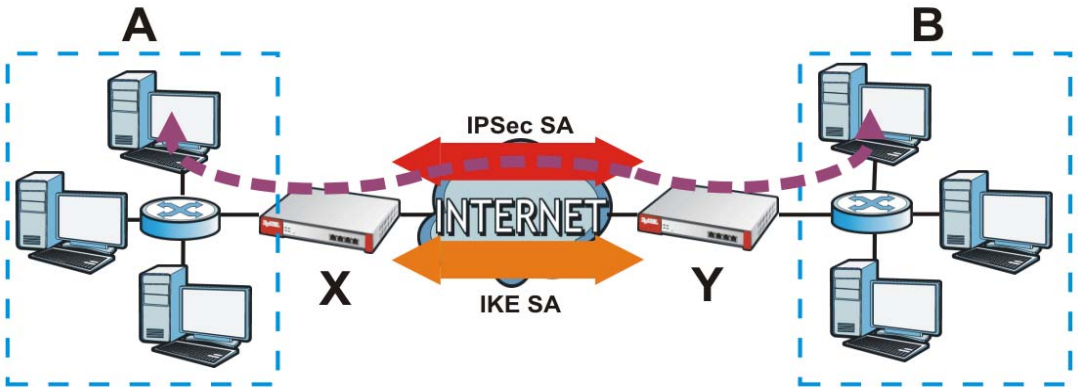
20.1.1 What You Can Do in this Chapter

- Use the **VPN Connection** screens (see Section 20.2 on page 285) to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).
- Use the **VPN Gateway** screens (see Section 20.2.1 on page 286) to manage the ZyWALL's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.
- Use the **VPN Concentrator** screens (see Section 20.4 on page 301) to combine several IPSec VPN connections into a single secure network.
- Use the **Configuration Provisioning** screen (see Section 20.5 on page 303) to set who can retrieve VPN rule settings from the ZyWALL using the ZyWALL IPSec VPN Client.

20.1.2 What You Need to Know

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 177 VPN: IKE SA and IPSec SA

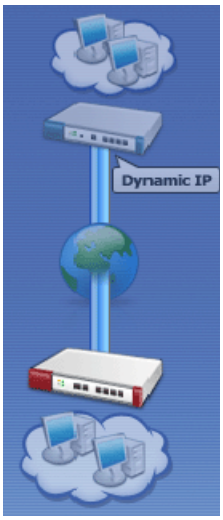


In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

Application Scenarios

The ZyWALL's application scenarios make it easier to configure your VPN connection settings.

Table 105 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)
			
Choose this if the remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this ZyWALL has a static IP address or a domain name.	Choose this if the remote IPSec router has a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This ZyWALL must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.	Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.	Choose this to connect to an IPSec server. This ZyWALL is the client (dial-in user). Client role ZyWALLs initiate IPSec VPN connections to a server role ZyWALL. This ZyWALL can have a dynamic IP address. The IPSec server doesn't configure this ZyWALL's IP address or the addresses of the devices behind it. Only this ZyWALL can initiate the VPN tunnel.

Finding Out More

- See Section 20.6 on page 305 for IPSec VPN background information.

20.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

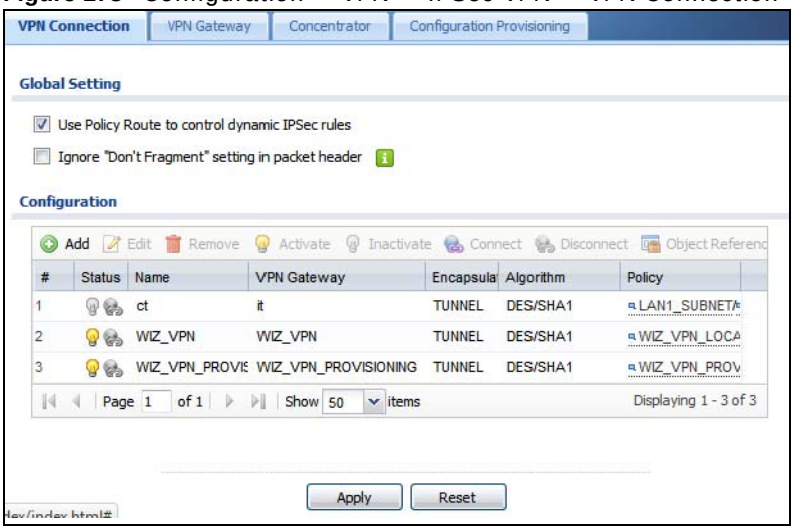
You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the ZyWALL uses as its IP address when it establishes the IKE SA. You should set up the interface first. See Chapter 7 on page 103.
- In a VPN gateway, you can enable extended authentication. If the ZyWALL is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the ZyWALL authenticates the remote IPSec router. See Chapter 31 on page 400.
- In a VPN gateway, the ZyWALL and remote IPSec router can use certificates to authenticate each other. Make sure the ZyWALL and the remote IPSec router will trust each other's certificates. See Chapter 33 on page 413.

20.2 The VPN Connection Screen

Click **Configuration > VPN > IPSec VPN** to open the **VPN Connection** screen. The **VPN Connection** screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 178 Configuration > VPN > IPSec VPN > VPN Connection



Each field is discussed in the following table. See Section 20.2.2 on page 292 and Section 20.2.1 on page 286 for more information.

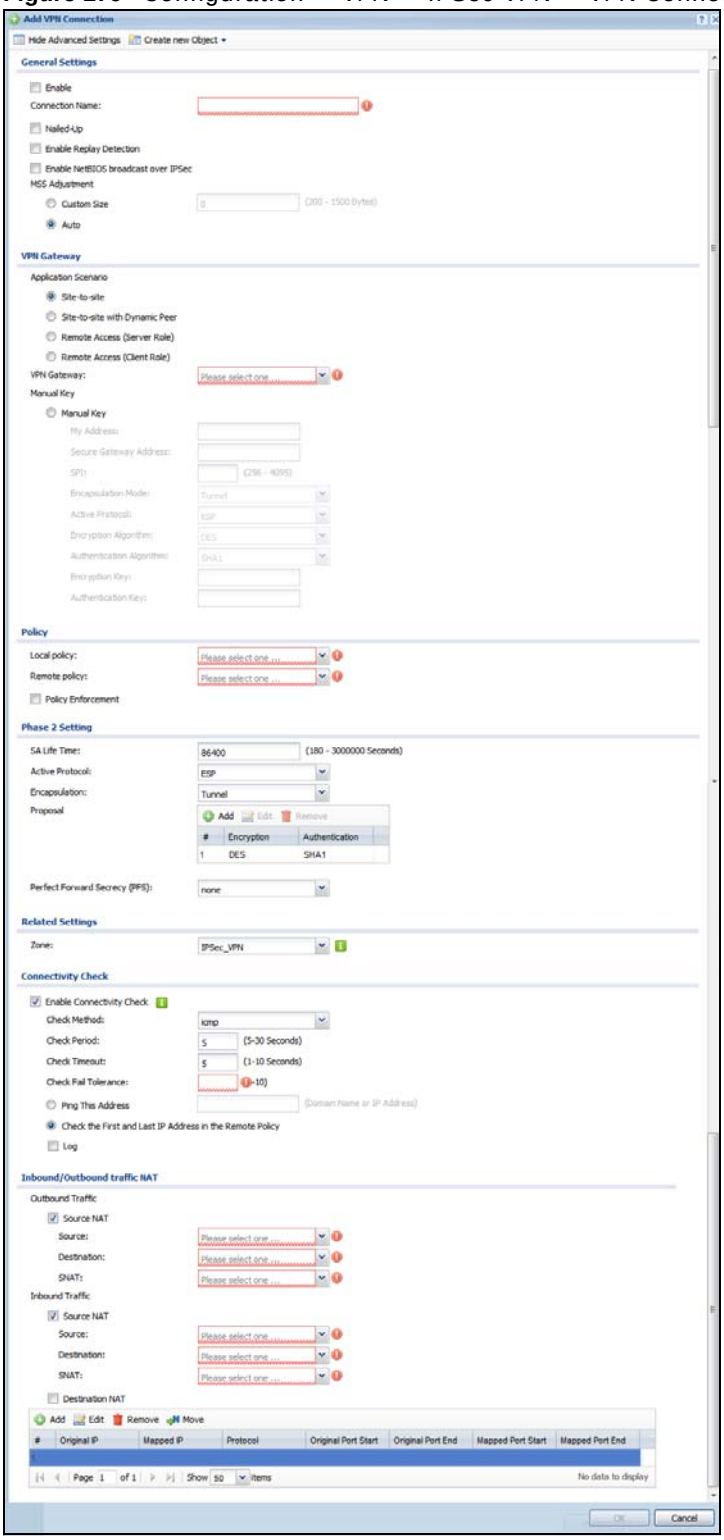
Table 106 Configuration > VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Use Policy Route to control dynamic IPSec rules	Select this to be able to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ZyWALL automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. Clear this to have the ZyWALL automatically obtain source and destination addresses for all dynamic IPSec rules.
Ignore "Don't Fragment" setting in packet header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the “don’t” fragment” bit in the IP header turned on. When you clear this the ZyWALL drops packets larger than the MTU that have the “don’t” fragment” bit in the header turned on.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an IPSec SA, select it and click **Connect**.
Disconnect	To disconnect an IPSec SA, select it and click **Disconnect**.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the associated VPN gateway(s). If there is no VPN gateway, this field displays “manual key”.
Encapsulation	This field displays what encapsulation the IPSec SA uses.
Algorithm	This field displays what encryption and authentication methods, respectively, the IPSec SA uses.
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.2.1 The VPN Connection Add/Edit (IKE) Screen

The **VPN Connection Add/Edit Gateway** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **Configuration > VPN Connection** screen (see Section 20.2 on page 285), and click either the **Add** icon or an **Edit** icon.

Figure 179 Configuration > VPN > IPSec VPN > VPN Connection > Edit (IKE)



Each field is described in the following table.

Table 107 Configuration > VPN > IPSec VPN > VPN Connection > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the ZyWALL to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this check box if you the ZyWALL to send NetBIOS (Network Basic Input/ Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
MSS Adjustment	Select **Custom Size** to set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection. Select **Auto** to have the ZyWALL automatically set the MSS for this VPN connection.
VPN Gateway	
Application Scenario	Select the scenario that best describes your intended VPN connection. **Site-to-site** - Choose this if the remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel. **Site-to-site with Dynamic Peer** - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. **Remote Access (Server Role)** - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. **Remote Access (Client Role)** - Choose this to connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel.
VPN Gateway	Select the VPN gateway this VPN connection is to use or select **Create Object** to add another VPN gateway for this VPN connection to use.
Manual Key	Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management. See Section 20.2.2 on page 292 for how to configure the manual key fields. Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.
Policy	
Local Policy	Select the address corresponding to the local network. Use **Create new Object** if you need to configure a new one.

Table 107 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Remote Policy	Select the address corresponding to the remote network. Use **Create new Object** if you need to configure a new one.
Policy Enforcement	Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks. Selecting this restricts who can use the VPN tunnel. The ZyWALL drops traffic with source and destination IP addresses that do not match the local and remote policy.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The ZyWALL automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and **Authentication** algorithm. Both **AH** and **ESP** increase processing requirements and latency (delay). The ZyWALL and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data. **Transport** - this mode only encrypts the data. The ZyWALL and remote IPSec router must use the same encapsulation.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the ZyWALL accepts from the remote IPSec router for negotiating the IPSec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.

Table 107 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than **MD5**, but it is also slower. The ZyWALL and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **none** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Related Settings	
Zone	Select the security zone into which to add this VPN connection policy. Any security rules or settings configured for the selected zone apply to this VPN connection policy.
Connectivity Check	The ZyWALL can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.
Check Method	Select how the ZyWALL checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the ZyWALL regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.
Check Port	This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the ZyWALL disconnects the VPN tunnel. The ZyWALL resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check this Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check the First and Last IP Address in the Remote Policy	Select this to have the ZyWALL check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.
Log	Select this to have the ZyWALL generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	

Table 107 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**.
Original Port Start / Original Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.

Table 107 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

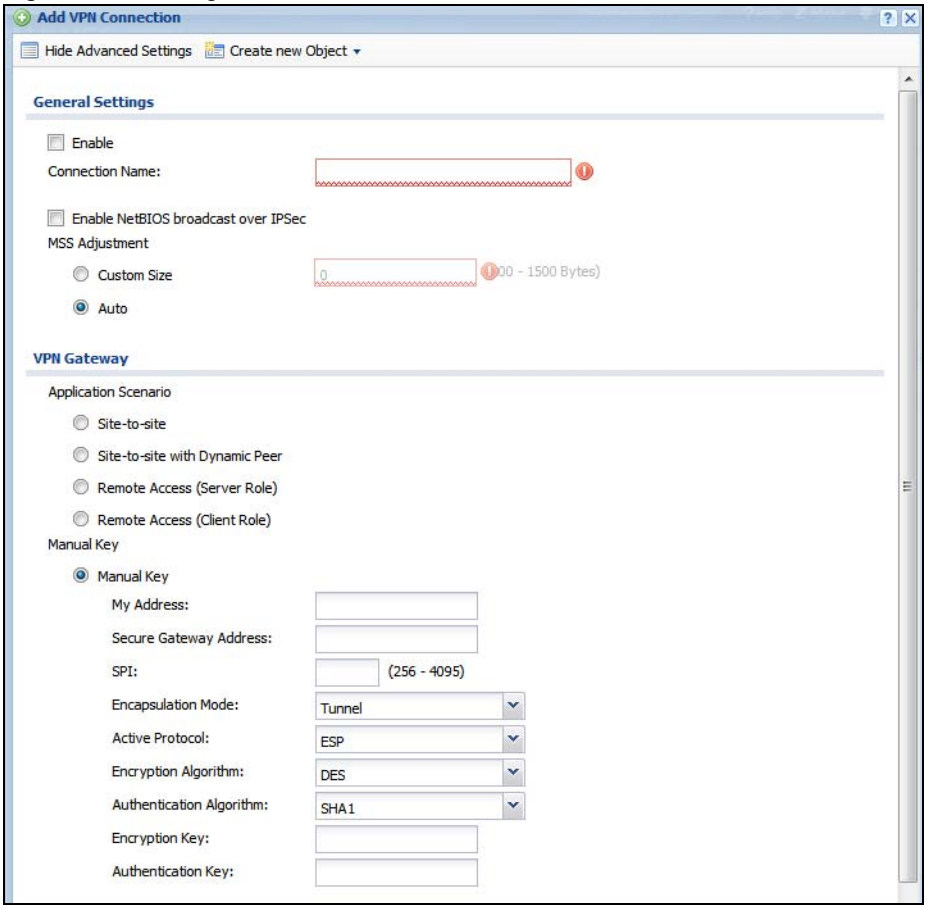
LABEL	DESCRIPTION
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

20.2.2 The VPN Connection Add/Edit Manual Key Screen

The **VPN Connection Add / Edit Manual Key** screen allows you to create a new VPN connection or edit an existing one using a manual key. This is useful if you have problems with IKE key management. To access this screen, go to the **VPN Connection** summary screen (see Section 20.2 on page 285), click either the **Add** icon or an existing manual key entry's **Edit** icon and click **Show Advanced Settings**. In the VPN Gateway section of the screen, select **Manual Key**.

Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.

Figure 180 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key



This table describes labels specific to manual key configuration. See Section 20.2 on page 285 for descriptions of the other fields.

Table 108 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key

LABEL	DESCRIPTION
Manual Key	
My Address	Type the IP address of the ZyWALL in the IPSec SA.
Secure Gateway Address	Type the IP address of the remote IPSec router in the IPSec SA.
SPI	Type a unique **SPI** (Security Parameter Index) between 256 and 4095. The SPI is used to identify the ZyWALL during authentication. The ZyWALL and remote IPSec router must use the same SPI.
Encapsulation Mode	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data **Transport** - this mode only encrypts the data. You should only select this if the IPSec SA is used for communication between the ZyWALL and remote IPSec router. If you select **Transport** mode, the ZyWALL automatically switches to **Tunnel** mode if the IPSec SA is not used for communication between the ZyWALL and remote IPSec router. In this case, the ZyWALL generates a log message for this change. The ZyWALL and remote IPSec router must use the same encapsulation.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication Algorithm**. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Algorithm** and **Authentication Algorithm**. The ZyWALL and remote IPSec router must use the same protocol.
Encryption Algorithm	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same algorithm and key. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than **MD5**, but it is also slower. The ZyWALL and remote IPSec router must use the same algorithm.

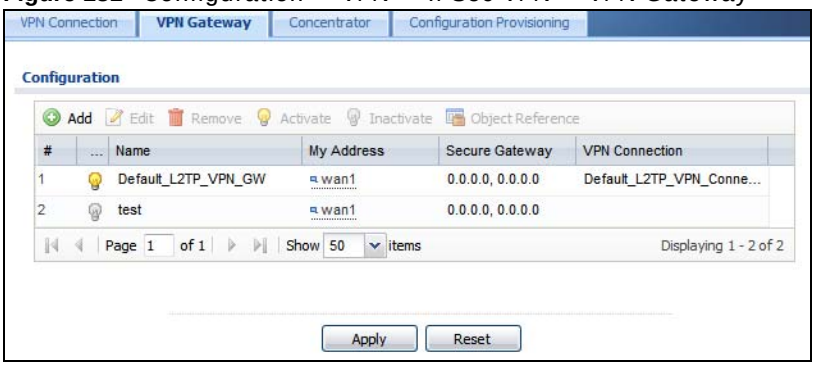
Table 108 Configuration > VPN > IPSec VPN > VPN Connection > Add > Manual Key (continued)

LABEL	DESCRIPTION
Encryption Key	This field is applicable when you select an **Encryption Algorithm**. Enter the encryption key, which depends on the encryption algorithm. **DES** - type a unique key 8-32 characters long **3DES** - type a unique key 24-32 characters long **AES128** - type a unique key 16-32 characters long **AES192** - type a unique key 24-32 characters long **AES256** - type a unique key 32 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same encryption key. The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ZyWALL only uses 12345678. The ZyWALL still stores the longer key.
Authentication Key	Enter the authentication key. The length depends on the authentication algorithm. **MD5** - type a unique key 16-20 characters long **SHA1** - type a unique key 20 characters long **SHA256** - type a unique key 32 characters long **SHA512** - type a unique key 64 characters long You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above. The remote IPSec router must have the same authentication key. The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 12345678901234567890 for a MD5 authentication key, the ZyWALL only uses 1234567890123456. The ZyWALL still stores the longer key.
OK	Click **OK** to save your settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

20.3 The VPN Gateway Screen

The **VPN Gateway** summary screen displays the IPSec VPN gateway policies in the ZyWALL, as well as the ZyWALL’s address, remote IPSec router’s address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway. To access this screen, click **Configuration > VPN** > **Network** > **IPSec VPN** > **VPN Gateway**. The following screen appears.

Figure 181 Configuration > VPN > IPSec VPN > VPN Gateway



Each field is discussed in the following table. See Section 20.3.1 on page 295 for more information.

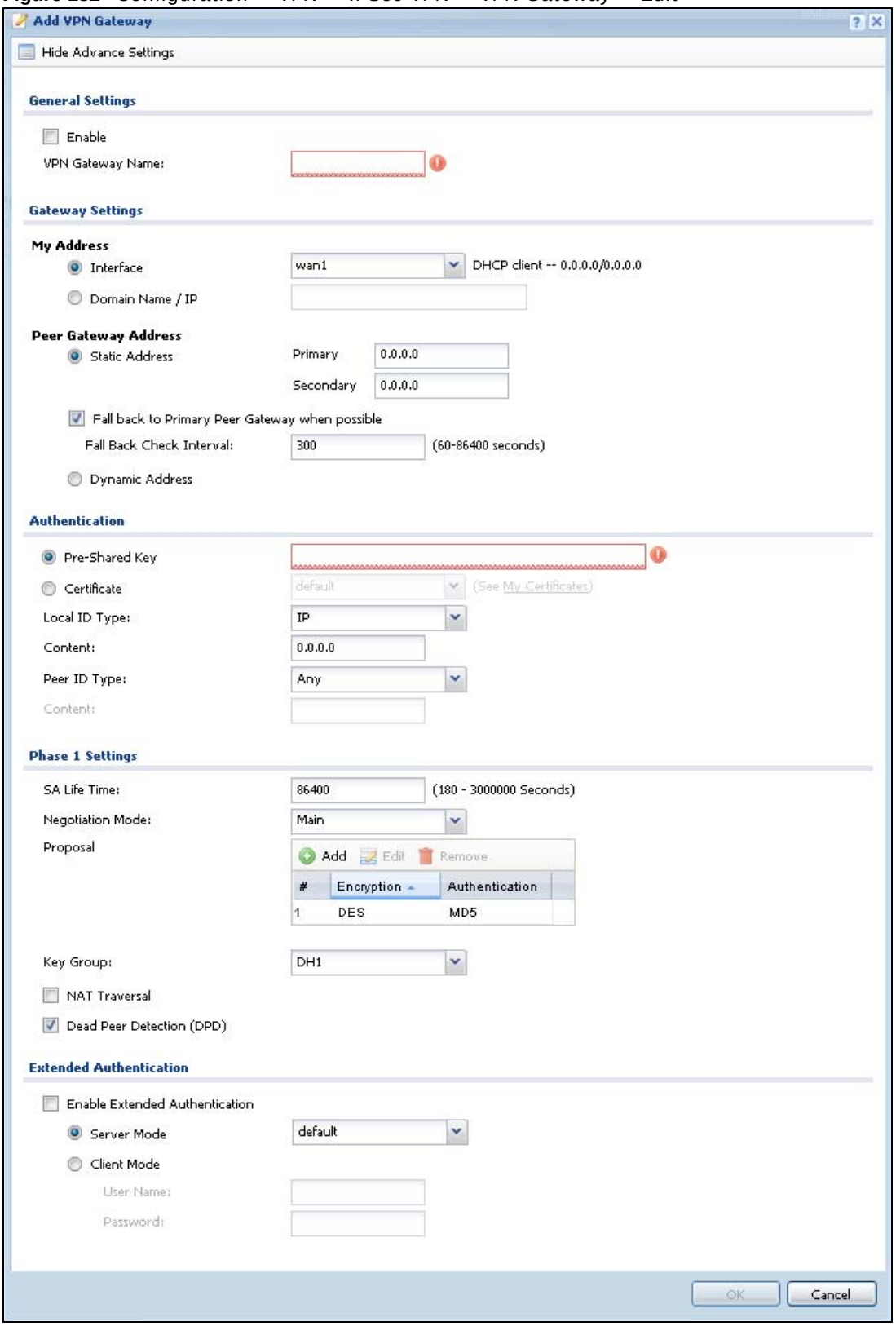
Table 109 Configuration > VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My address	This field displays the interface or a domain name the ZyWALL uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.3.1 The VPN Gateway Add/Edit Screen

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the **VPN Gateway summary** screen (see Section 20.3 on page 294), and click either the **Add** icon or an **Edit** icon.

Figure 182 Configuration > VPN > IPSec VPN > VPN Gateway > Edit



Each field is described in the following table.

Table 110 Configuration > VPN > IPSec VPN > VPN Gateway > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Gateway Settings	
My Address	Select how the IP address of the ZyWALL in the IKE SA is defined. If you select **Interface**, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the ZyWALL in the IKE SA is the IP address of the interface. If you select **Domain Name / IP**, enter the domain name or the IP address of the ZyWALL. The IP address of the ZyWALL in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the ZyWALL accept IPSec requests destined for any interface address on the ZyWALL.
Peer Gateway Address	Select how the IP address of the remote IPSec router in the IKE SA is defined. Select **Static Address** to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the ZyWALL to try if it cannot establish an IKE SA with the first one. **Fall back to Primary Peer Gateway when possible**: When you select this, if the connection to the primary address goes down and the ZyWALL changes to using the secondary connection, the ZyWALL will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the ZyWALL changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the **Fallback Check Interval** field, set how often to check if the primary address is available. Select **Dynamic Address** if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Authentication	Note: The ZyWALL and remote IPSec router must use the same authentication method to establish the IKE SA.
Pre-Shared Key	Select this to have the ZyWALL and remote IPSec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be: • alphanumeric characters or ,;.|`~!@#$%^&*()_+\{}':./<>=-" • pairs of hexadecimal (0-9, A-F) characters, preceded by “0x”. Type “0x” at the beginning of a hexadecimal key. For example, "0x0123456789ABCDEF" is in hexadecimal format; “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The ZyWALL and remote IPSec router must use the same pre-shared key.

Table 110 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Certificate	Select this to have the ZyWALL and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the ZyWALL uses to identify itself to the remote IPsec router. This certificate is one of the certificates in **My Certificates**. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA. Note: The IPSec routers must trust each other's certificates. The ZyWALL uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
Local ID Type	This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the ZyWALL during authentication. Choices are: **IP** - the ZyWALL is identified by an IP address **DNS** - the ZyWALL is identified by a domain name **E-mail** - the ZyWALL is identified by the string specified in this field
Content	This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Type the identity of the ZyWALL during authentication. The identity depends on the **Local ID Type**. **IP** - type an IP address; if you type 0.0.0.0, the ZyWALL uses the IP address specified in the **My Address** field. This is not recommended in the following situations: • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Local ID Type**. **DNS** - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. **E-mail** - the ZyWALL is identified by the string you specify here; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: **IP** - the remote IPSec router is identified by an IP address **DNS** - the remote IPSec router is identified by a domain name **E-mail** - the remote IPSec router is identified by the string specified in this field **Any** - the ZyWALL does not check the identity of the remote IPSec router If the ZyWALL and remote IPSec router use certificates, there is one more choice. **Subject Name** - the remote IPSec router is identified by the subject name in the certificate

Table 110 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Content	This field is disabled if the **Peer ID Type** is **Any**. Type the identity of the remote IPSec router during authentication. The identity depends on the **Peer ID Type**. If the ZyWALL and remote IPSec router do not use certificates, **IP** - type an IP address; see the note at the end of this description. **DNS** - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. **E-mail** - the remote IPSec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the ZyWALL and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. **IP** - subject alternative name field; see the note at the end of this description. **DNS** - subject alternative name field **E-mail** - subject alternative name field **Subject Name** - subject name (maximum 255 ASCII characters, including spaces) Note: If **Peer ID Type** is **IP**, please read the rest of this section. If you type 0.0.0.0, the ZyWALL uses the IP address specified in the **Secure Gateway Address** field. This is not recommended in the following situations: • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Peer ID Type**.
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the ZyWALL and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are **Main** - this encrypts the ZyWALL's and remote IPSec router's identities but takes more time to establish the IKE SA **Aggressive** - this is faster but does not encrypt the identities The ZyWALL and the remote IPSec router must use the same negotiation mode.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the ZyWALL accepts from the remote IPSec router for negotiating the IKE SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 110 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than **MD5**, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the ZyWALL and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.
Dead Peer Detection (DPD)	Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec router. If the remote IPSec router responds, the ZyWALL transmits the data. If the remote IPSec router does not respond, the ZyWALL shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 20.2.1 on page 286).
More Settings/Less Settings	Click this button to show or hide the **Extended Authentication** fields.
Extended Authentication	When multiple IPSec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel's security settings, each still has to provide a unique user name and password.
Enable Extended Authentication	Select this if one of the routers (the ZyWALL or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the ZyWALL authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the ZyWALL authenticates this information.

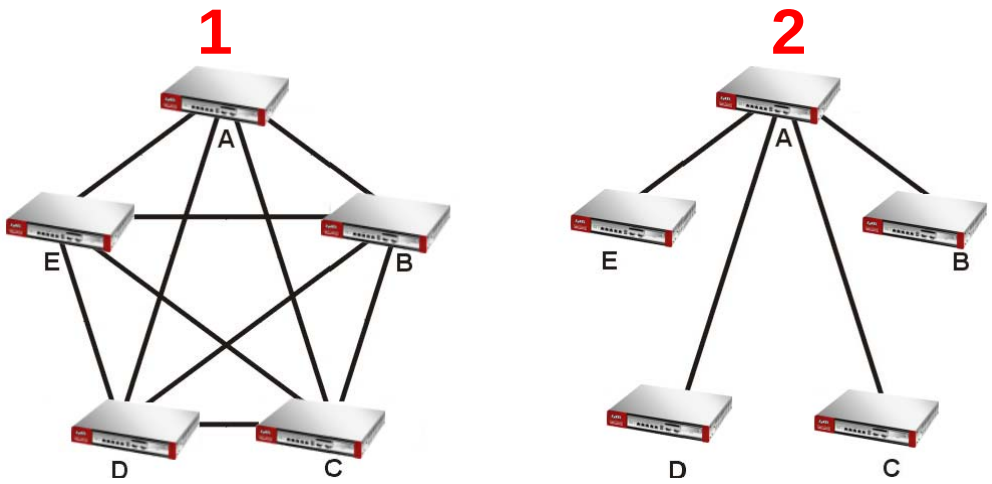
Table 110 Configuration > VPN > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Client Mode	Select this radio button if the ZyWALL provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**.
User Name	This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the user name the ZyWALL sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the password the ZyWALL sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
OK	Click **OK** to save your settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

20.4 VPN Concentrator

A VPN concentrator combines several IPSec VPN connections into one secure network.

Figure 183 VPN Topologies (Fully Meshed and Hub and Spoke)



In a fully-meshed VPN topology (**1** in the figure), there is a VPN connection between every pair of routers. In a hub-and-spoke VPN topology (**2** in the figure), there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

A VPN concentrator reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

However a VPN concentrator is not for every situation. The hub router is a single failure point, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). There is also more burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

20.4.1 VPN Concentrator Requirements and Suggestions

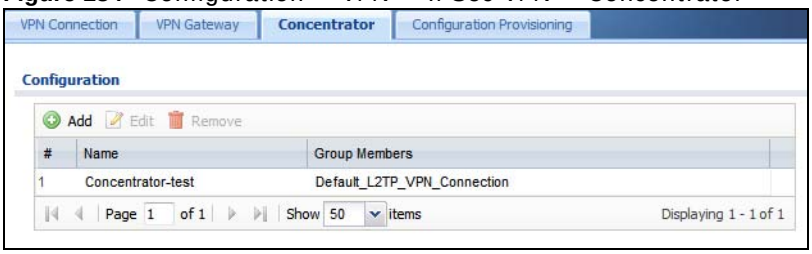
Consider the following when using the VPN concentrator.

- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your firewall rules can still block VPN packets.

20.4.2 VPN Concentrator Screen

The **VPN Concentrator** summary screen displays the VPN concentrators in the ZyWALL. To access this screen, click **Configuration > VPN** > **IPSec VPN** > **Concentrator**.

Figure 184 Configuration > VPN > IPSec VPN > Concentrator



Each field is discussed in the following table. See Section 20.4.3 on page 302 for more information.

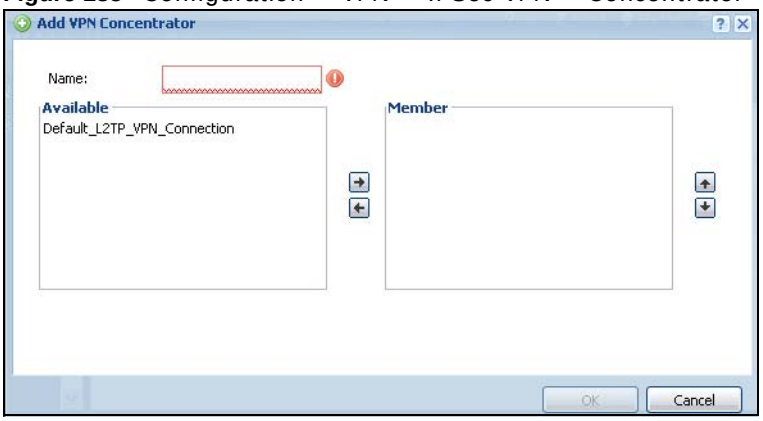
Table 111 Configuration > VPN > IPSec VPN > Concentrator

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Group Members	These are the VPN connection policies that are part of the VPN concentrator.

20.4.3 The VPN Concentrator Add/Edit Screen

Use the **VPN Concentrator Add/Edit** screen to create or edit a VPN concentrator. To access this screen, go to the **VPN Concentrator summary** screen (see Section 20.4 on page 301), and click either the **Add** icon or an **Edit** icon.

Figure 185 Configuration > VPN > IPSec VPN > Concentrator > Edit



Each field is described in the following table.

Table 112 VPN > IPSec VPN > Concentrator > Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member	Select the concentrator's IPSec VPN connection policies. Note: You must disable policy enforcement in each member. See Section 20.2.1 on page 286. IPSec VPN connection policies that do not belong to a VPN concentrator appear under **Available**. Select any VPN connection policies that you want to add to the VPN concentrator and click the right arrow button to add them. The VPN concentrator's member VPN connections appear under **Member**. Select any VPN connections that you want to remove from the VPN concentrator, and click the left arrow button to remove them.
OK	Click **OK** to save your changes in the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

20.5 ZyWALL IPSec VPN Client Configuration Provisioning

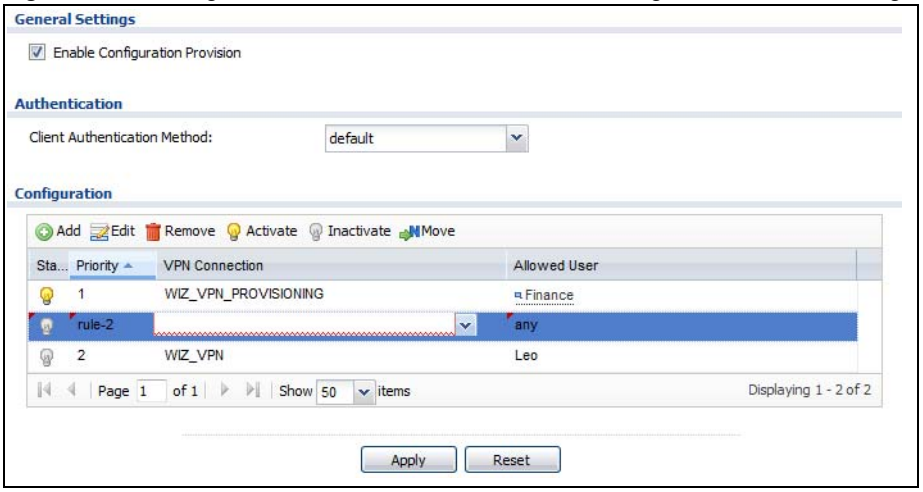
Use the **Configuration > VPN > IPSec VPN > Configuration Provisioning** screen to configure who can retrieve VPN rule settings from the ZyWALL using the ZyWALL IPSec VPN Client. In the ZyWALL IPSec VPN Client, you just need to enter the IP address of the ZyWALL to get all the VPN rule settings automatically. You do not need to manually configure all rule settings in the ZyWALL IPSec VPN client.

VPN rules for the ZyWALL IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- **AH** active protocol
- **NULL** encryption
- **SHA512** authentication
- A subnet or range remote policy

In the ZyWALL **Quick Setup** wizard, you can use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that will not violate these restrictions.

Figure 186 Configuration > VPN > IPSec VPN > Configuration Provisioning



Each field is discussed in the following table.

Table 113 Configuration > VPN > IPSec VPN > Configuration Provisioning

LABEL	DESCRIPTION
Enable Configuration Provisioning	Select this for users to be able to retrieve VPN rule settings using the ZyWALL IPSec VPN client.
Client Authentication Method	Choose how users should be authenticated. They can be authenticated using the local database on the ZyWALL or an external authentication database such as LDAP, Active Directory or RADIUS. **default** is a method you configured in **Object > Auth Method.** You may configure multiple methods there. If you choose the local database on the ZyWALL, then configure users using the **Object > User/Group** screen. If you choose LDAP, Active Directory or RADIUS authentication servers, then configure users on the respective server.
Configuration	When you add or edit a configuration provisioning entry, you are allowed to set the **VPN Connection** and **Allowed User** fields. Duplicate entries are not allowed. You cannot select the same **VPN Connection** and **Allowed User** pair in a new entry if the same pair exists in a previous entry. You can bind different rules to the same user, but the ZyWALL will only allow VPN rule setting retrieval for the first match found.
Add	Click **Add** to bind a configured VPN rule to a user or group. Only that user or group may then retrieve the specified VPN rule settings. If you click **Add** without selecting an entry in advance then the new entry appears as the first entry. Entry order is important as the ZyWALL searches entries in the order listed here to find a match. After a match is found, the ZyWALL stops searching. If you want to add an entry as number three for example, then first select entry 2 and click **Add**. To reorder an entry, use **Move**.
Edit	Select an existing entry and click **Edit** to change its settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**. Make sure that **Enable Configuration Provisioning** is also selected.
Inactivate	To turn off an entry, select it and click **Inactivate**.

Table 113 Configuration > VPN > IPSec VPN > Configuration Provisioning (continued)

LABEL	DESCRIPTION
Move	Use **Move** to reorder a selected entry. Select an entry, click **Move**, type the number where the entry should be moved, press <ENTER>, then click **Apply**.
Status	This icon shows if the entry is active (yellow) or not (gray). VPN rule settings can only be retrieved when the entry is activated (and **Enable Configuration Provisioning** is also selected).
Priority	Priority shows the order of the entry in the list. Entry order is important as the ZyWALL searches entries in the order listed here to find a match. After a match is found the ZyWALL stops searching.
VPN Connection	This field shows all configured VPN rules that match the rule criteria for the ZyWALL IPSec VPN client. Select a rule to bind to the associated user or group.
Allowed User	Select which user or group of users is allowed to retrieve the associated VPN rule settings using the ZyWALL IPSec VPN client. A user may belong to a number of groups. If entries are configured for different groups, the ZyWALL will allow VPN rule setting retrieval based on the first match found. Users of type **admin** or **limited-admin** are not allowed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.6 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 308. Main mode is used in various examples in the rest of this section.

IP Addresses of the ZyWALL and Remote IPSec Router

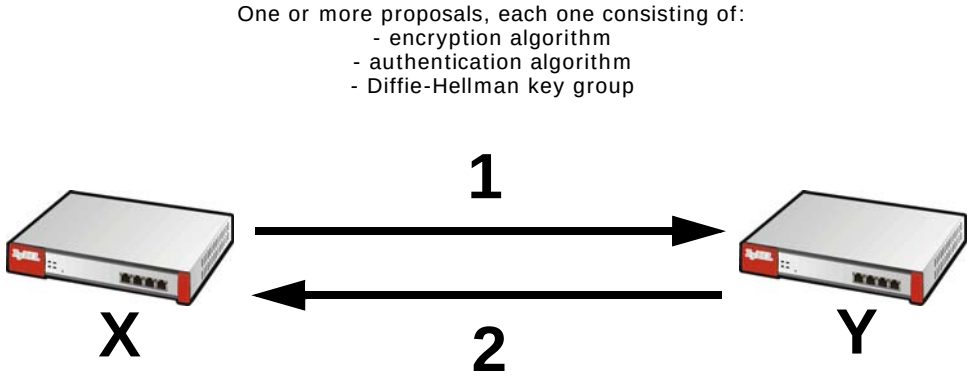
To set up an IKE SA, you have to specify the IP addresses of the ZyWALL and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your ZyWALL might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the ZyWALL does not know the IP address of the remote IPSec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 187 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals, the ZyWALL and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some ZyWALLs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most ZyWALLs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

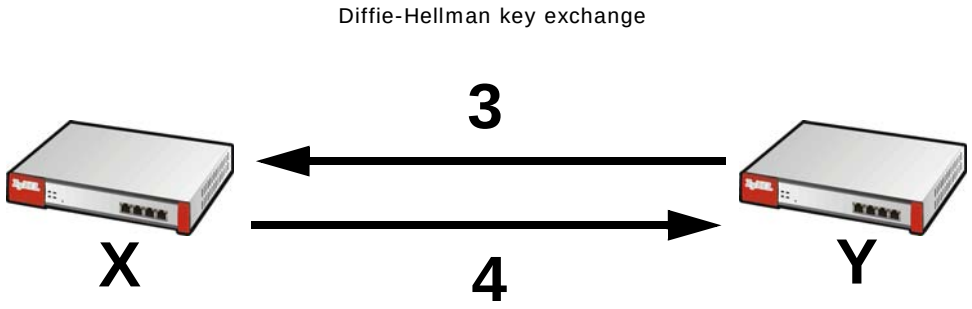
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 307 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 188 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



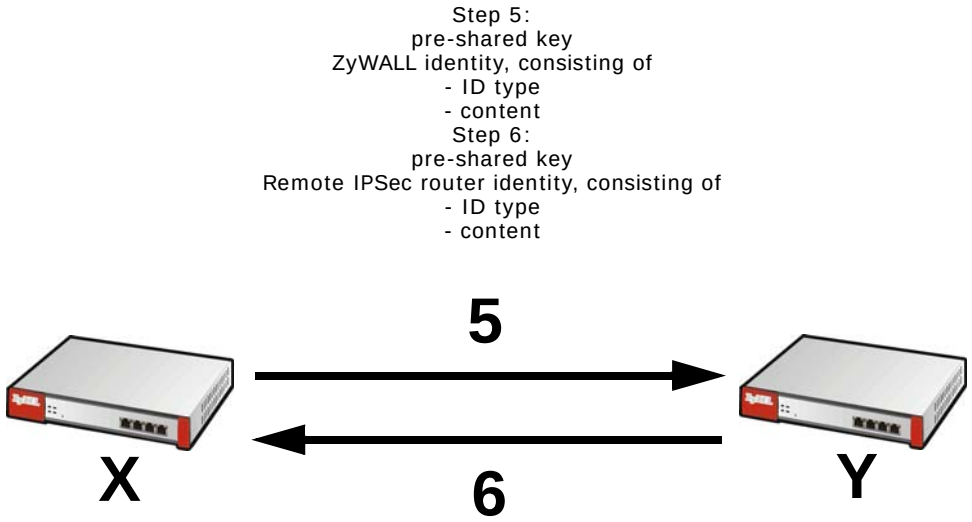
DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Authentication

Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

Figure 189 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)



You have to create (and distribute) a pre-shared key. The ZyWALL and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the ZyWALL's or remote IPSec router's properties.

The ZyWALL and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The ZyWALL's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in Table 114 on page 308, the ZyWALL and the remote IPSec router authenticate each other successfully. In contrast, in Table 115 on page 308, the ZyWALL and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 114 VPN Example: Matching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 115 VPN Example: Mismatching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the ZyWALL to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your ZyWALL provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The ZyWALL sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3 - 4: The ZyWALL and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

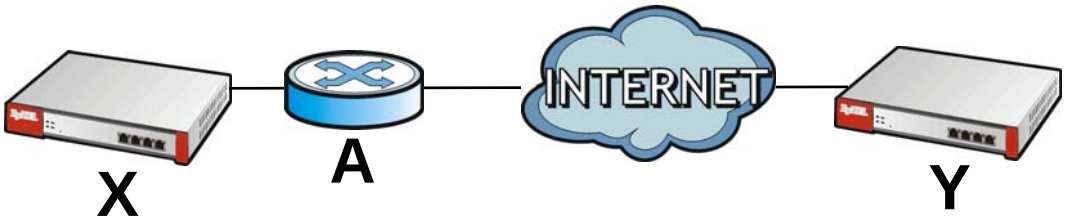
Steps 5 - 6: Finally, the ZyWALL and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 190 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 310 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the ZyWALL and remote IPSec router first.

IPSec SA Overview

Once the ZyWALL and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the ZyWALL, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The ZyWALL and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

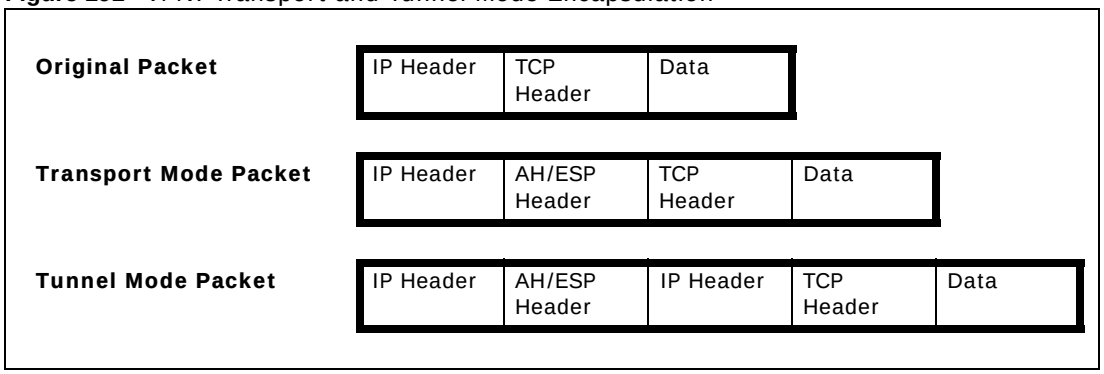
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ZyWALL and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The ZyWALL and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 191 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 306), except that you also have the choice whether or not the ZyWALL and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the ZyWALL and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

Additional Topics for IPSec SA

This section provides more information about IPSec SA in your ZyWALL.

IPSec SA using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ZyWALL and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

IPSec SA Proposal using Manual Keys

In an IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyWALL and remote IPSec router use.

Note: The ZyWALL and remote IPSec router must use the same encryption key and authentication key.

Authentication and the Security Parameter Index (SPI)

For authentication, the ZyWALL and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The ZyWALL and remote IPSec router must use the same SPI.

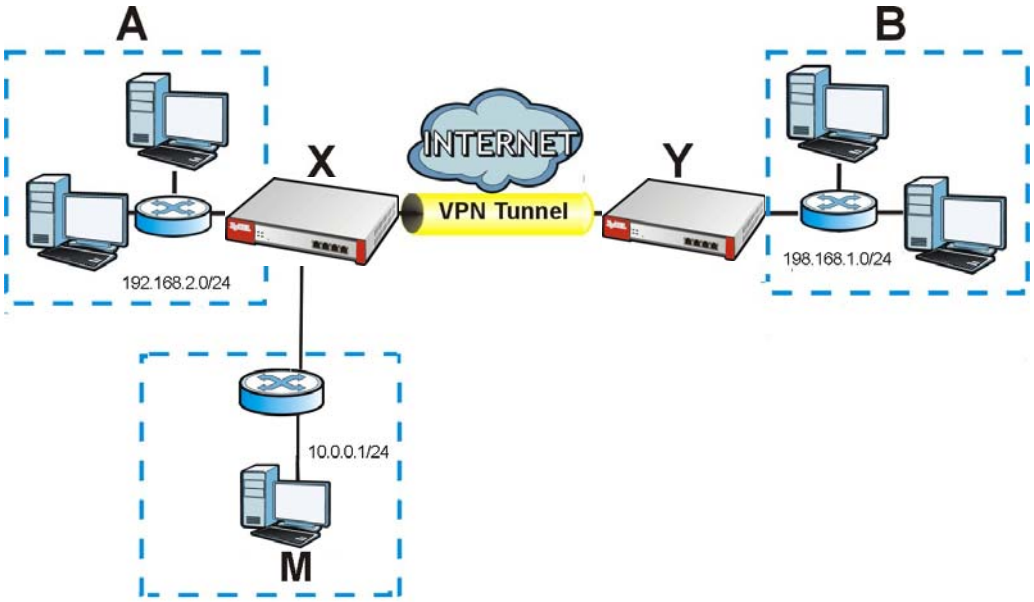
NAT for Inbound and Outbound Traffic

The ZyWALL can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 192 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the ZyWALL route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 192 on page 313, you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPSec router may not route messages for computer **M** through the IPSec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the ZyWALL to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 192 on page 313, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The ZyWALL checks these rules similar to the way it checks rules for a firewall. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 192 on page 313, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

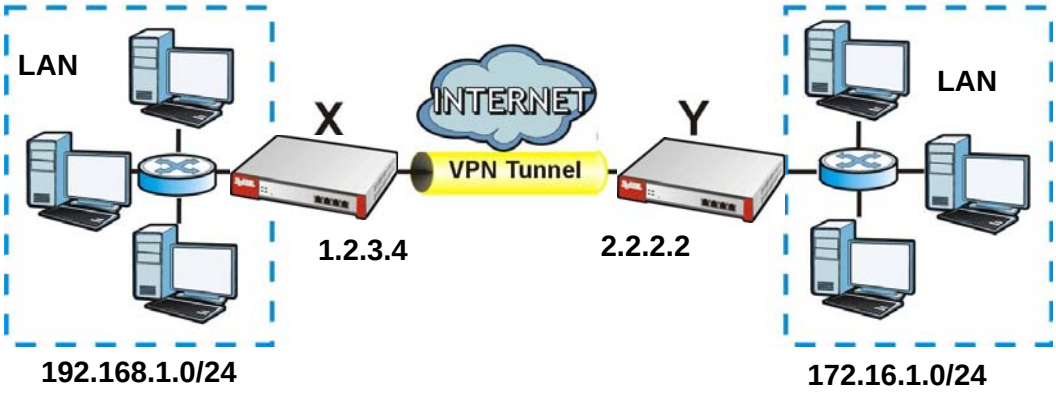
- Mapped IP - the translated destination address; in Figure 192 on page 313, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

IPSec VPN Example

Here is an example of configuring a site-to-site IPSec VPN.

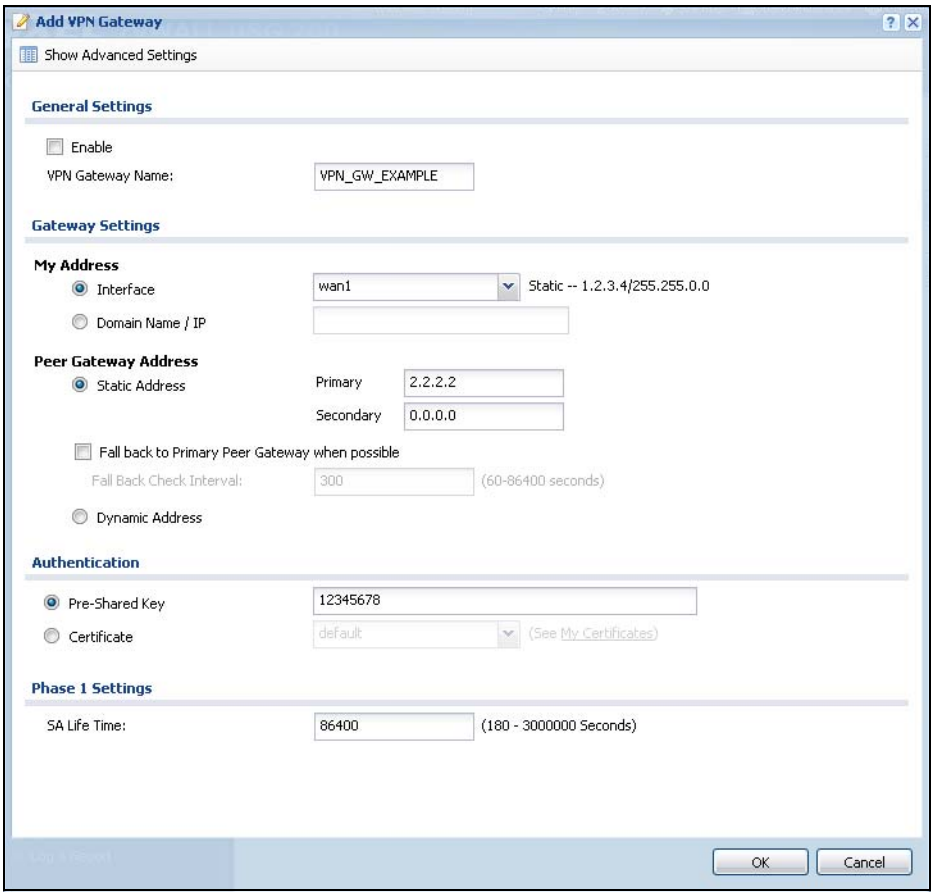
Figure 193 IPSec VPN Example



ZyWALL **X** uses 1.2.3.4 as its public address, and remote IPSec router **Y** uses 2.2.2.2. Create the VPN tunnel between the ZyWALL's LAN subnet (192.168.1.0/24) and the LAN subnet behind the peer IPSec router (172.16.1.0/24).

Set Up the VPN Gateway that Manages the IKE SA

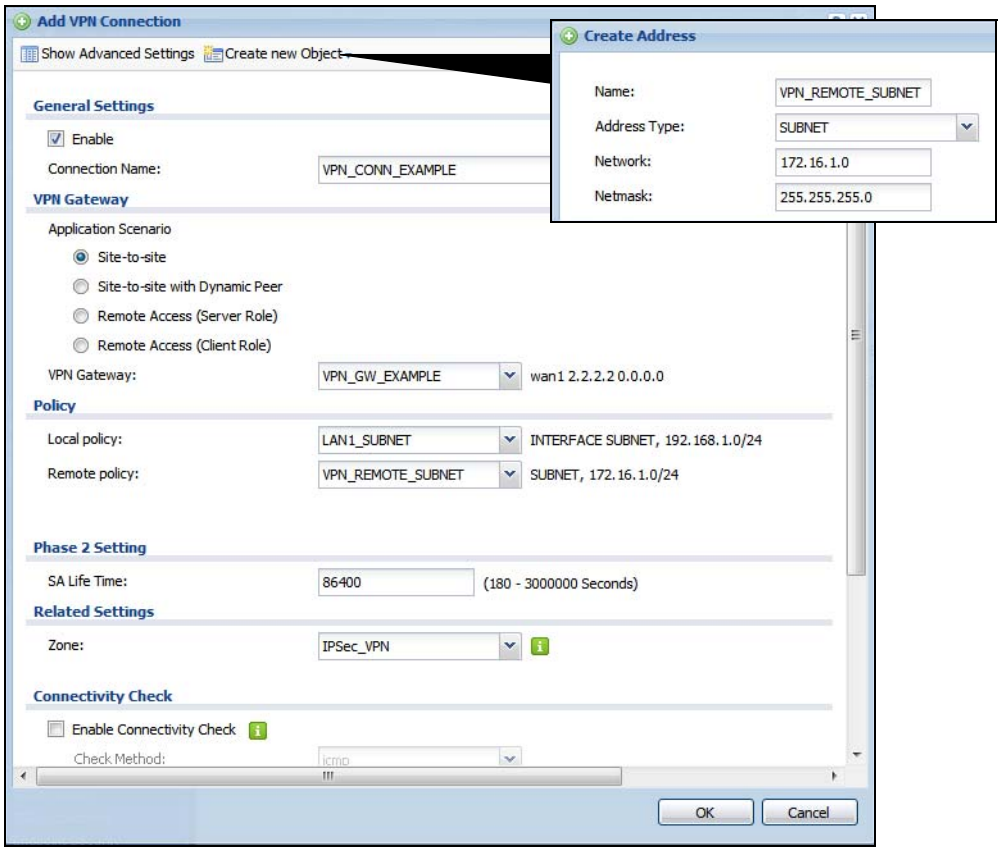
In **Configuration > VPN > IPSec VPN > VPN Gateway > Add**, enable the VPN gateway and name it (VPN_GW_EXAMPLE here). Set **My Address** to **Interface** and select a WAN interface. Set **Peer Gateway Address** to **Static Address** and enter the remote IPSec router's public IP address (2.2.2.2 here) as the **Primary**. Set **Authentication** to **Pre-Shared Key** and enter 12345678. Click **OK**.



Set Up the VPN Connection that Manages the IPSec SA

1 In **Configuration > VPN > IPSec VPN > VPN Connection > Add**, click **Create New Object > Address** to create an address object for the remote network. Set the **Address Type** to **SUBNET**, the **Network** field to 172.16.1.0, and the **Netmask** to 255.255.255.0.

2 Enable the VPN connection and name it ("VPN_CONN_EXAMPLE"). Set **VPN Gateway** to **Site-to-site** and select the VPN gateway you configured (**VPN_GW_EXAMPLE**). Set **Local Policy** to **LAN1_SUBNET** and **Remote Policy** to **VPN_REMOTE_SUBNET** for the remote. Click **OK**.


Add VPN Connection
Show Advanced Settings
Create new Object
General Settings
Enable
Connection Name:
VPN_CONN_EXAMPLE
VPN Gateway
Application Scenario
Site-to-site
Site-to-site with Dynamic Peer
Remote Access (Server Role)
Remote Access (Client Role)
VPN Gateway:
VPN_GW_EXAMPLE
wan1 2.2.2.2 0.0.0.0
Policy
Local policy:
LAN1_SUBNET
INTERFACE SUBNET, 192.168.1.0/24
Remote policy:
VPN_REMOTE_SUBNET
SUBNET, 172.16.1.0/24
Phase 2 Setting
SA Life Time:
86400
(180 - 3000000 Seconds)
Related Settings
Zone:
IPSec_VPN
Connectivity Check
Enable Connectivity Check
Check Method:
icmp
OK
Cancel
Create Address
Name:
VPN_REMOTE_SUBNET
Address Type:
SUBNET
Network:
172.16.1.0
Netmask:
255.255.255.0

21

SSL VPN

21.1 Overview

Use SSL VPN to allow users to use a web browser for secure remote user login. The remote users do not need a VPN router or VPN client software.

21.1.1 What You Can Do in this Chapter

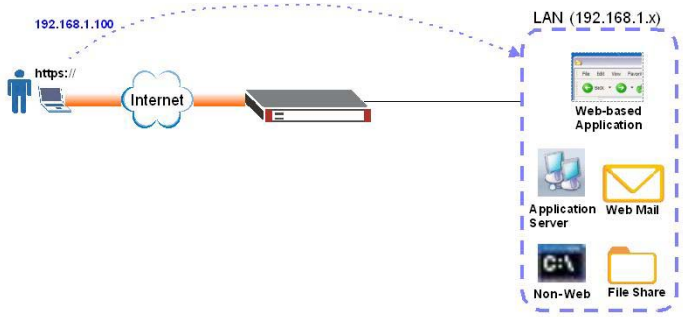
- Use the **VPN > SSL VPN > Access Privilege** screens (see Section 21.2 on page 318) to configure SSL access policies.
- Use the Click **VPN > SSL VPN** > **Global Setting** screen (see Section 21.3 on page 322) to set the IP address of the ZyWALL (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

21.1.2 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

Figure 194 Network Access Mode: Full Tunnel Mode



SSL Access Policy

An SSL access policy allows the ZyWALL to perform the following tasks:

- limit user access to specific applications or file sharing server on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the ZyWALL automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 116 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Configure a user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Configure address objects for the IP addresses of the DNS and WINS servers that the ZyWALL sends to the VPN connection users.
VPN Network	Address	Configure an address object to specify which network segment users are allowed to access through a VPN connection.

You cannot delete an object that is referenced by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

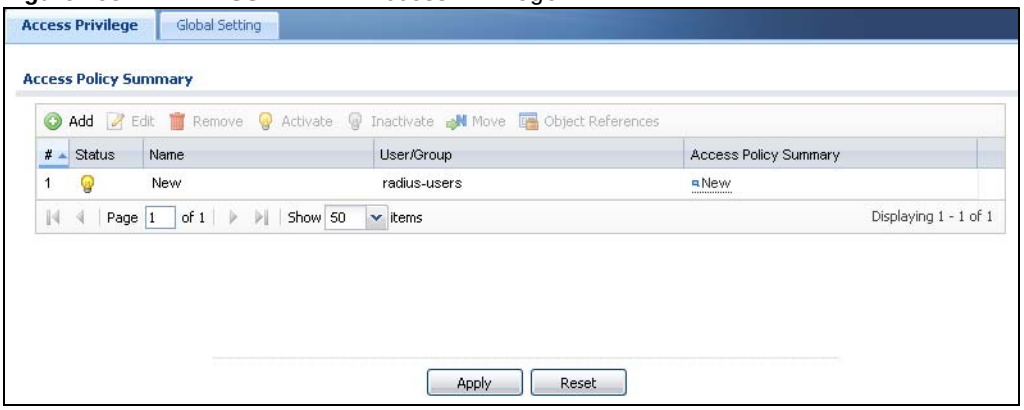
Finding Out More

- See Section 21.4 on page 324 for an SSL VPN example.
- See Chapter 35 on page 432 for details on SSL application objects.

21.2 The SSL Access Privilege Screen

Click **VPN > SSL VPN** to open the **Access Privilege** screen. This screen lists the configured SSL access policies.

Figure 195 VPN > SSL VPN > Access Privilege



The following table describes the labels in this screen.

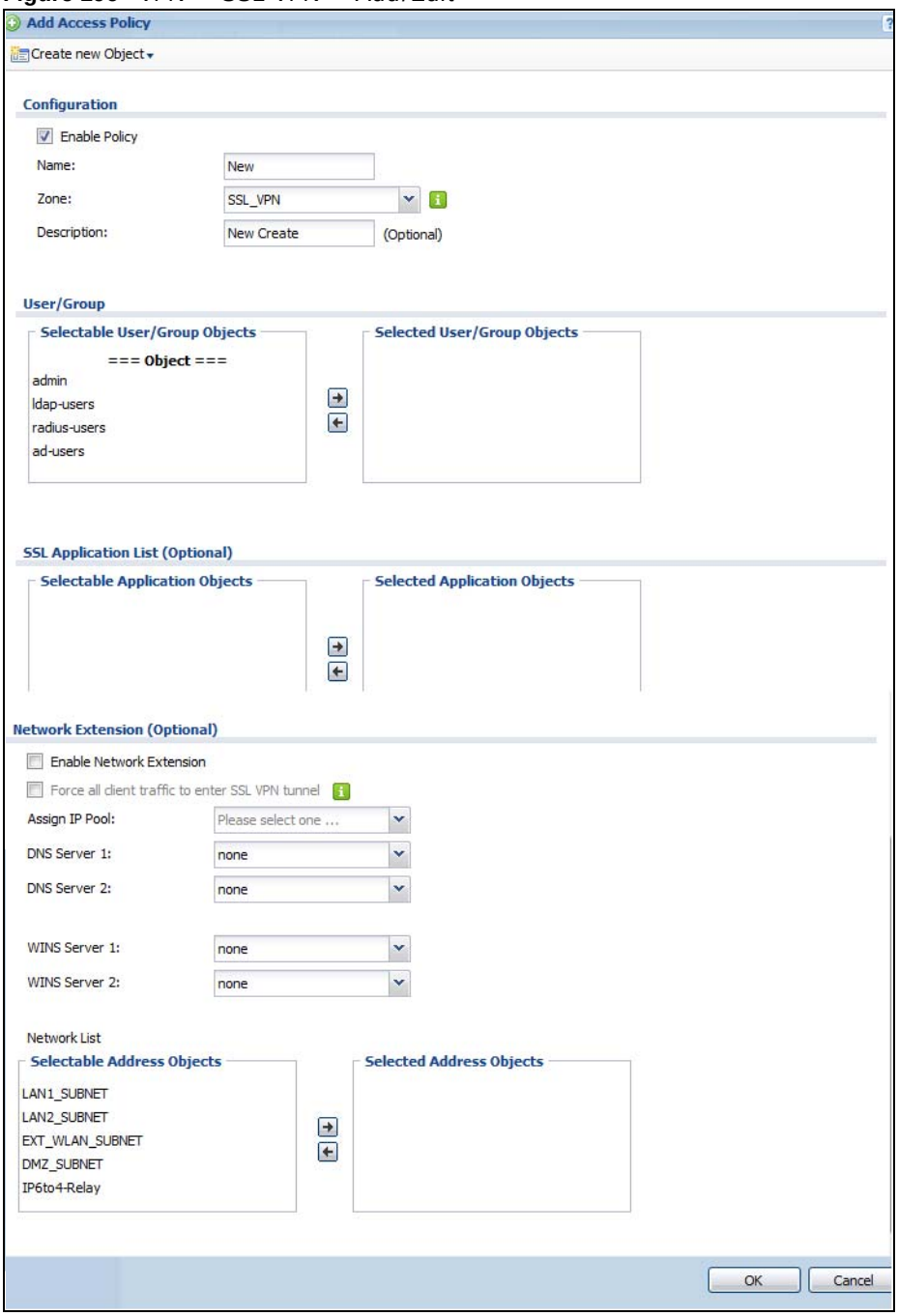
Table 117 VPN > SSL VPN > Access Privilege

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive name of the SSL access policy for identification purposes.
User/Group	This field displays the user account or user group name(s) associated to an SSL access policy. This field displays up to three names.
Access Policy Summary	This field displays details about the SSL application object this policy uses including its name, type, and address.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to discard all changes.

21.2.1 The SSL Access Policy Add/Edit Screen

To create a new or edit an existing SSL access policy, click the **Add** or **Edit** icon in the **Access Privilege** screen.

Figure 196 VPN > SSL VPN > Add/Edit



The following table describes the labels in this screen.

Table 118 VPN > SSL VPN > Access Privilege > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable Policy	Select this option to activate this SSL access policy.

Table 118 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
Name	Enter a descriptive name to identify this policy. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.
Zone	Select the zone to which to add this SSL access policy. You use zones to apply security settings such as firewall and remote management.
Description	Enter additional information about this SSL access policy. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
User/Group	The **Selectable User/Group Objects** list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet. To associate a user or user group to this SSL access policy, select a user account or user group and click the right arrow button to add to the **Selected User/Group Objects** list. You can select more than one name. To remove a user or user group, select the name(s) in the **Selected User/Group Objects** list and click the left arrow button. Note: Although you can select admin and limited-admin accounts in this screen, they are reserved for device configuration only. You cannot use them to access the SSL VPN portal.
SSL Application List (Optional)	The **Selectable Application Objects** list displays the name(s) of the SSL application(s) you can select for this SSL access policy. To associate an SSL application to this SSL access policy, select a name and click the right arrow button to add to the **Selected Application Objects** list. You can select more than one application. To remove an SSL application, select the name(s) in the **Selected Application Objects** list and click the left arrow button. Note: To allow access to shared files on a Windows 7 computer, within Windows 7 you must enable sharing on the folder and also go to the **Network and Sharing Center**’s **Advanced sharing settings** and turn on the current network profile’s file and printer sharing.
Network Extension (Optional)	
Enable Network Extension	Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. This includes access to resources not supported by SSL application objects. For example this lets users Telnet to the internal network even though the ZyWALL does not have SSL application objects for Telnet. Clear this option to disable this feature. Users can only access the applications as defined by the VPN tunnel’s selected SSL application settings and the remote user computers are not made to be a part of the local network.
Force all client traffic to SSL VPN tunnel	Select this to send all traffic from the SSL VPN clients through the SSL VPN tunnel. This replaces the default gateway of the SSL VPN clients with the SSL VPN gateway.
Assign IP Pool	Define a separate pool of IP addresses to assign to the SSL users. Select it here. The SSL VPN IP pool cannot overlap with IP addresses on the ZyWALL's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN **Network List**.
DNS/WINS Server 1..2	Select the name of the DNS or WINS server whose information the ZyWALL sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.

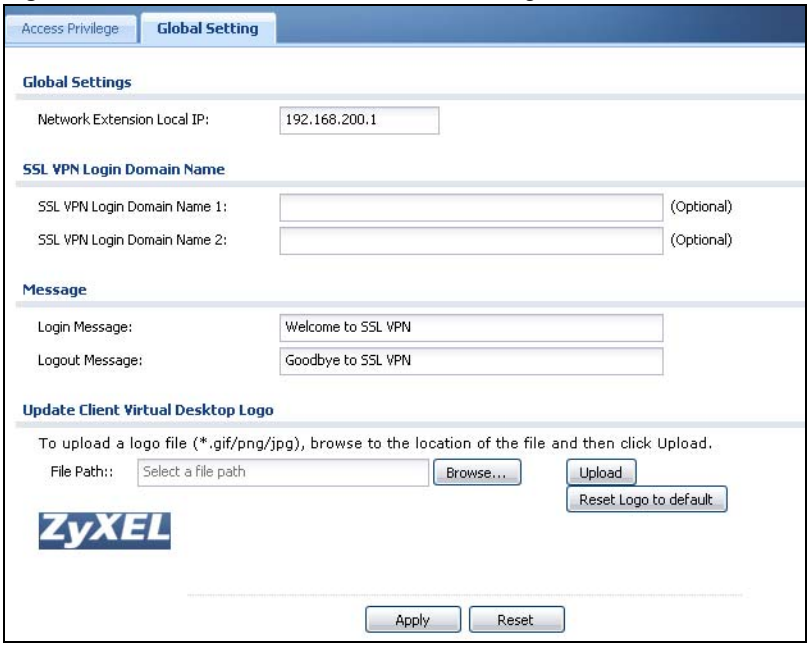
Table 118 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
Network List	To allow user access to local network(s), select a network name in the **Selectable Address Objects** list and click the right arrow button to add to the **Selected Address Objects** list. You can select more than one network. To block access to a network, select the network name in the **Selected Address Objects** list and click the left arrow button.
OK	Click **OK** to save the changes and return to the main **Access Privilege** screen.
Cancel	Click **Cancel** to discard all changes and return to the main **Access Privilege** screen.

21.3 The SSL Global Setting Screen

Click **VPN > SSL VPN** and click the **Global Setting** tab to display the following screen. Use this screen to set the IP address of the ZyWALL (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

Figure 197 VPN > SSL VPN > Global Setting



The following table describes the labels in this screen.

Table 119 VPN > SSL VPN > Global Setting

LABEL	DESCRIPTION
Global Setting	
Network Extension Local IP	Specify the IP address of the ZyWALL (or a gateway device) for full tunnel mode SSL VPN access. Leave this field to the default settings unless it conflicts with another interface.
SSL VPN Login Domain Name	

Table 119 VPN > SSL VPN > Global Setting (continued)

LABEL	DESCRIPTION
SSL VPN Login Domain Name 1/ 2	Specify a full domain name for users to use for SSL VPN login. The domain name must be registered to one of the ZyWALL's IP addresses or be one of the ZyWALL's DDNS entries. You can specify up to two domain names so you could use one domain name for each of two WAN ports. For example, www.zyxel.com is a fully qualified domain name where "www" is the host. The ZyWALL displays the normal login screen without the button for logging into the Web Configurator.
Message	
Login Message	Specify a message to display on the screen when a user logs in and an SSL VPN connection is established successfully. You can enter up to 60 characters (0-9, a-z, A-Z, '()+,/:=?;!*#@$_%-") with spaces allowed.
Logout Message	Specify a message to display on the screen when a user logs out and the SSL VPN connection is terminated successfully. You can enter up to 60 characters (0-9, a-z, A-Z, '()+,/:=?;!*#@$_%-") with spaces allowed.
Update Client Virtual Desktop Logo	You can upload a graphic logo to be displayed on the web browser on the remote user computer. The ZyXEL company logo is the default logo. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.
Browse	Click **Browse** to locate the graphic file on your computer.
Upload	Click **Upload** to transfer the specified graphic file from your computer to the ZyWALL.
Reset Logo to Default	Click **Reset Logo to Default** to display the ZyXEL company logo on the remote user's web browser.
Apply	Click **Apply** to save the changes and/or start the logo file upload process.
Reset	Click **Reset** to return the screen to its last-saved settings.

21.3.1 How to Upload a Custom Logo

Follow the steps below to upload a custom logo to display on the remote user SSL VPN screens.

1 Click **VPN > SSL VPN** and click the **Global Setting** tab to display the configuration screen.

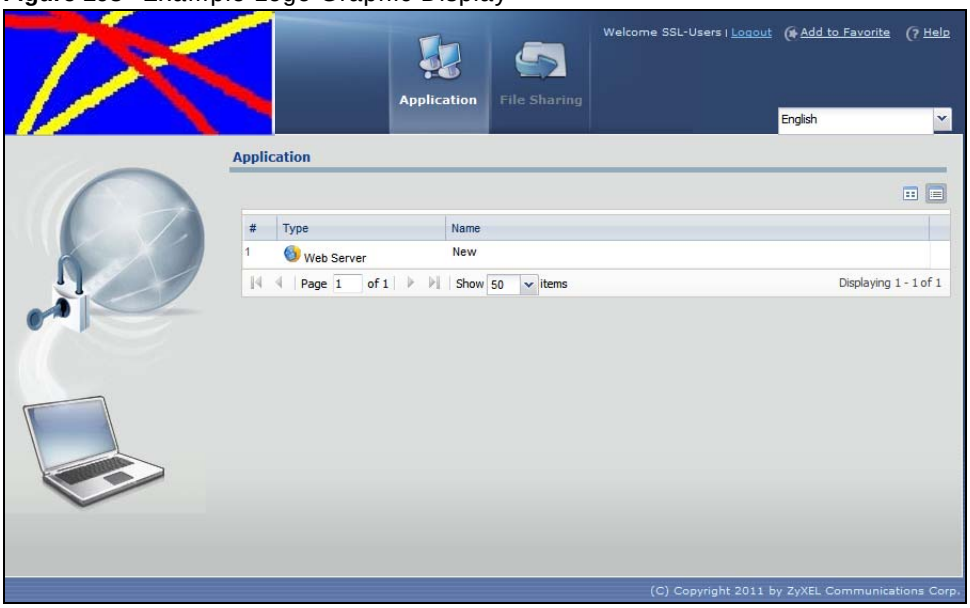
2 Click **Browse** to locate the logo graphic. Make sure the file is in GIF, JPG, or PNG format.

3 Click **Apply** to start the file transfer process.

4 Log in as a user to verify that the new logo displays properly.

The following shows an example logo on the remote user screen.

Figure 198 Example Logo Graphic Display

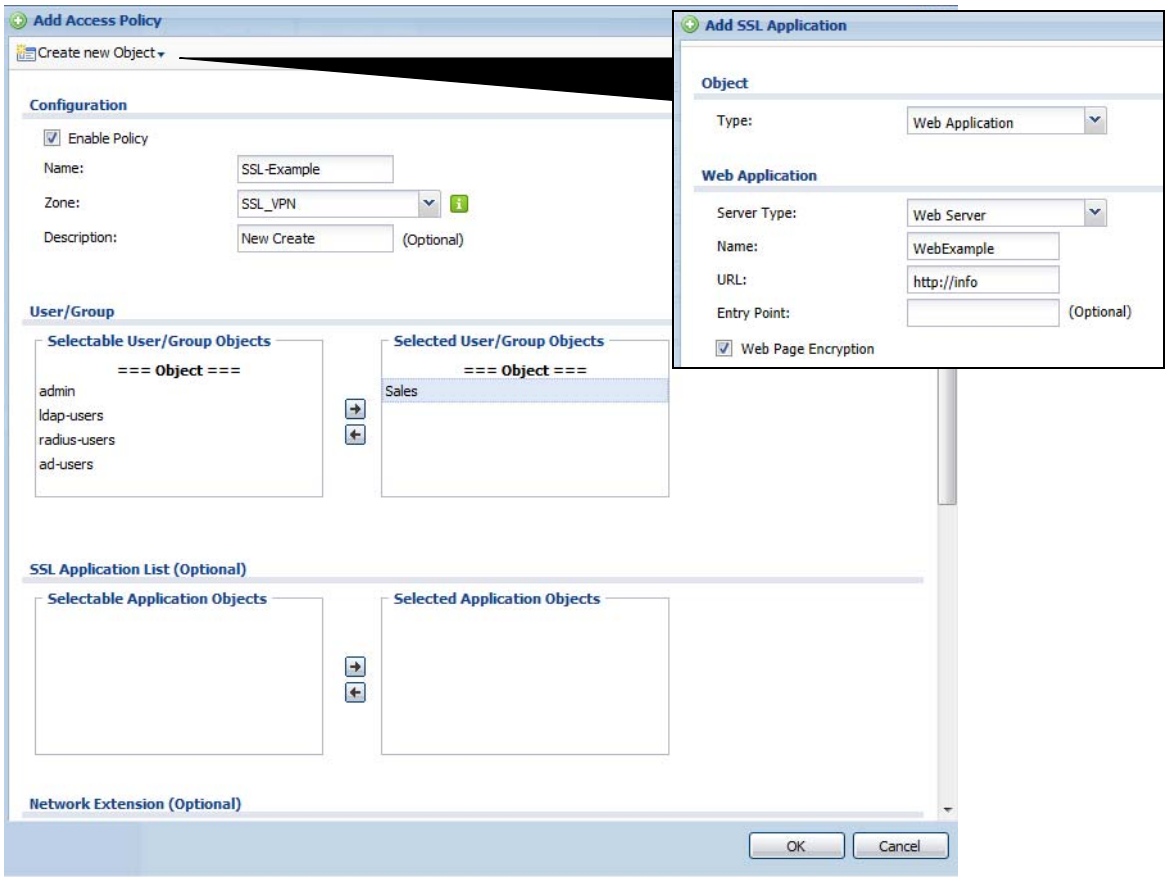


21.4 SSL VPN Example

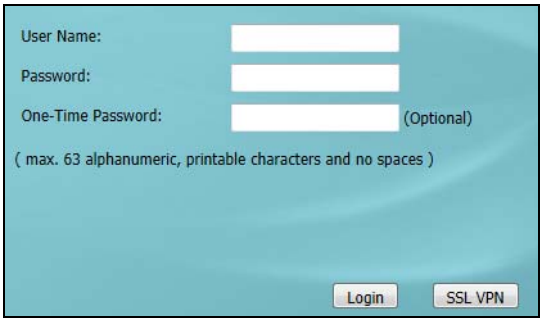
This example uses SSL VPN to let remote users securely access the internal http://info website.

1 Click **Configuration > VPN > SSL VPN > Access Privilege > Add** and click **Create New Object > Application** to create an SSL application object. Set the **Type** to **Web Application**, the **Server Type** to **Web Server**, and the **URL** to http://info. Select **Web Page Encryption** to prevent users from saving the web content.

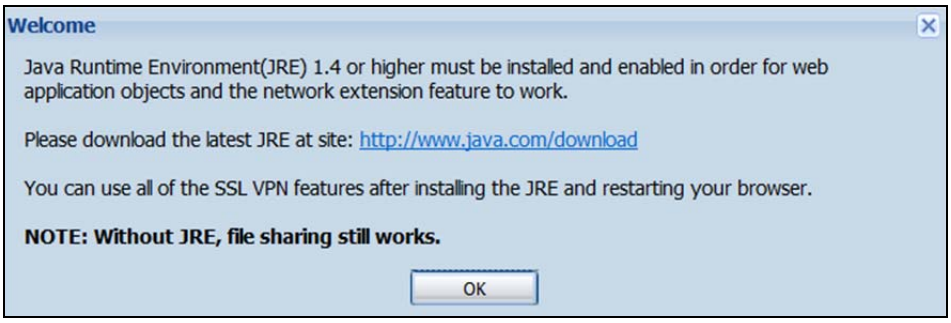
2 Enable the policy. Enter a descriptive name in the **Name** field (“SSL-Example” here). Select the users to which to give access (the Sales user group here). Select the SSL application object you created (“WebExample” here). Click **OK**.



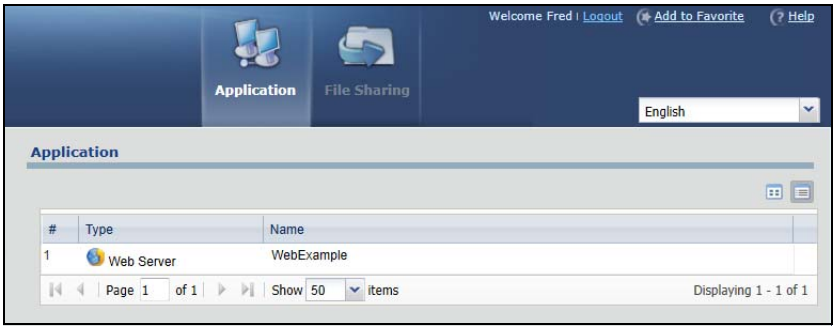
3 Display the ZyWALL's login screen, enter your user account information (the user name and password), and click **SSL VPN** to establish an SSL VPN connection.



4 Your computer starts establishing a secure connection to the ZyWALL after the login. This may take up to two minutes. If you get a message about needing Java, download and install it and restart your browser and re-login. If a certificate warning screen displays, click **OK**, **Yes** or **Continue**.


Welcome
Java Runtime Environment(JRE) 1.4 or higher must be installed and enabled in order for web application objects and the network extension feature to work.
Please download the latest JRE at site: http://www.java.com/download
You can use all of the SSL VPN features after installing the JRE and restarting your browser.
NOTE: Without JRE, file sharing still works.
OK

5 The client portal screen displays after the connection is up. In this example, click the **Web Server** link to go to http://info.



If the user account is not included in an SSL VPN access policy, the ZyWALL redirects the user to the user aware screen.

For more information on user portal screens, refer to Chapter 22 on page 327.

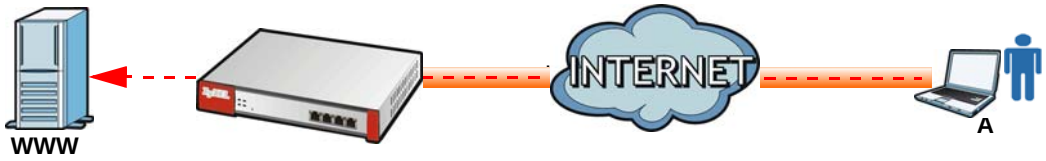
22

SSL User Screens

22.1 Overview

This chapter introduces the remote user SSL VPN screens. The following figure shows a network example where a remote user (**A**) logs into the ZyWALL from the Internet to access the web server (**WWW**) on the local network.

Figure 199 Network Example



22.1.1 What You Need to Know

The ZyWALL can use SSL VPN to provide secure connections to network resources such as applications, files, intranet sites or e-mail through a web-based interface and using Microsoft Outlook Web Access (OWA).

Network Resource Access Methods

As a remote user, you can access resources on the local network using one of the following methods.

- Using a supported web browser

  Once you have successfully logged in through the ZyWALL, you can access intranet sites, web-based applications, or web-based e-mails using one of the supported web browsers.
- Using the ZyWALL SecuExtender client

  Once you have successfully logged into the ZyWALL, if the SSL VPN access policy has network extension enabled the ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer. With the ZyWALL SecuExtender, you can access network resources, remote desktops and manage files as if you were on the local network. See Chapter 23 on page 341 for more on the ZyWALL SecuExtender.

System Requirements

Here are the browser and computer system requirements for remote user access.

- Windows 7 (32 or 64-bit), Vista (32 or 64-bit), 2003 (32-bit), XP (32-bit), or 2000 (32-bit)
- Internet Explorer 7 and above or Firefox 1.5 and above

- Using RDP requires Internet Explorer
- Sun's Runtime Environment (JRE) version 1.6 or later installed and enabled.

Required Information

A remote user needs the following information from the network administrator to log in and access network resources.

- the domain name or IP address of the ZyWALL
- the login account user name and password
- if also required, the user name and/or password to access the network resource

Certificates

The remote user's computer establishes an HTTPS connection to the ZyWALL to access the login screen. If instructed by your network administrator, you must install or import a certificate (provided by the ZyWALL or your network administrator).

Finding Out More

See Chapter 21 on page 317 for how to configure SSL VPN on the ZyWALL.

22.2 Remote SSL User Login

This section shows you how to access and log into the network through the ZyWALL. Example screens for Internet Explorer are shown.

1 Open a web browser and enter the web site address or IP address of the ZyWALL. For example, "http://sslvpn.mycompany.com".

Figure 200 Enter the Address in a Web Browser



2 Click **OK** or **Yes** if a security screen displays.

Figure 201 Login Security Screen


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

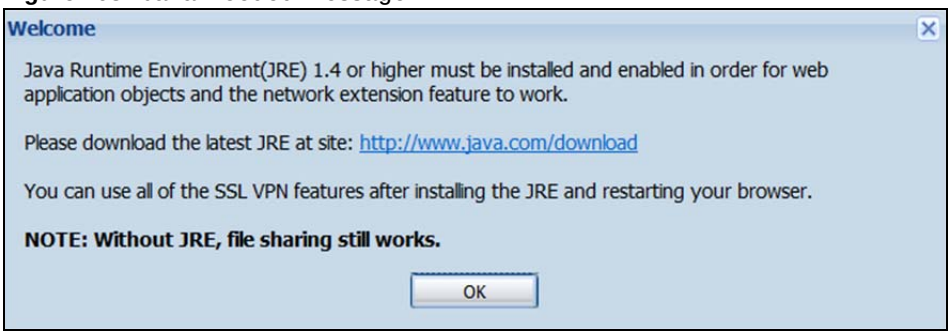
3 A login screen displays. Enter the user name and password of your login account. If a token password is also required, enter it in the **One-Time Password** field. Click **SSL VPN** to log in and establish an SSL VPN connection to the network to access network resources.

Figure 202 Login Screen



4 Your computer starts establishing a secure connection to the ZyWALL after a successful login. This may take up to two minutes. If you get a message about needing Java, download and install it and restart your browser and re-login. If a certificate warning screen displays, click **OK**, **Yes** or **Continue**.

Figure 203 Java Needed Message


Welcome
Java Runtime Environment(JRE) 1.4 or higher must be installed and enabled in order for web application objects and the network extension feature to work.
Please download the latest JRE at site: http://www.java.com/download
You can use all of the SSL VPN features after installing the JRE and restarting your browser.
NOTE: Without JRE, file sharing still works.
OK

5 The ZyWALL tries to install the SecuExtender client. As shown next, you may have to click some pop-ups to get your browser to allow the installation.

Figure 204 ActiveX Object Installation Blocked by Browser

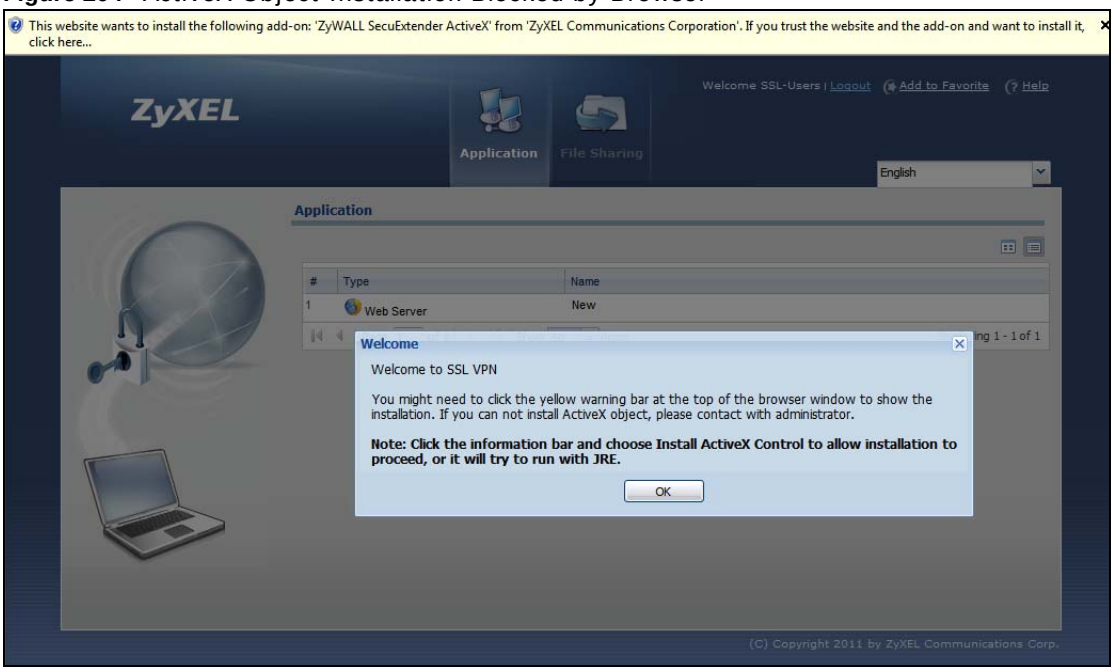

This website wants to install the following add-on: 'ZyWALL SecuExtender ActiveX' from 'ZyXEL Communications Corporation'. If you trust the website and the add-on and want to install it, click here...
ZyXEL
Application
File Sharing
Welcome SSL-Users | Logout
Add to Favorite
Help
English
Application
Type Name
1 Web Server New
Welcome
Welcome to SSL VPN
You might need to click the yellow warning bar at the top of the browser window to show the installation. If you can not install ActiveX object, please contact with administrator.
Note: Click the information bar and choose Install ActiveX Control to allow installation to proceed, or it will try to run with JRE.
OK
(C) Copyright 2011 by ZyXEL Communications Corp.

Figure 205 SecuExtender Blocked by Internet Explorer


Internet Explorer - Security Warning
Do you want to install this software?
Name: ZyWALL SecuExtender ActiveX
Publisher: ZyXEL Communications Corporation
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

6 The ZyWALL tries to run the “ssltun” application. You may need to click something to get your browser to allow this. In Internet Explorer, click **Run**.

Figure 206 SecuExtender Progress


Warning - Security
The application's digital signature has been verified.
Do you want to run the application?
Name: ssltun
Publisher: ZyXEL Communications Corporation
From: https://172.23.31.19
Always trust content from this publisher.
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

7 Click **Next** to use the setup wizard to install the SecuExtender client on your computer.

Figure 207 SecuExtender Progress


ZyWALL SecuExtender Setup
ZyXEL
Welcome to the ZyWALL SecuExtender Setup Wizard
The Setup Wizard will install ZyWALL SecuExtender on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.
< Back
Next >
Cancel

8 If a screen like the following displays, click **Continue Anyway** to finish installing the SecuExtender client on your computer.

Figure 208 Installation Warning


Hardware Installation
The software you are installing for this hardware:
ZyXEL ZyWALL SecuExtender Adapter
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

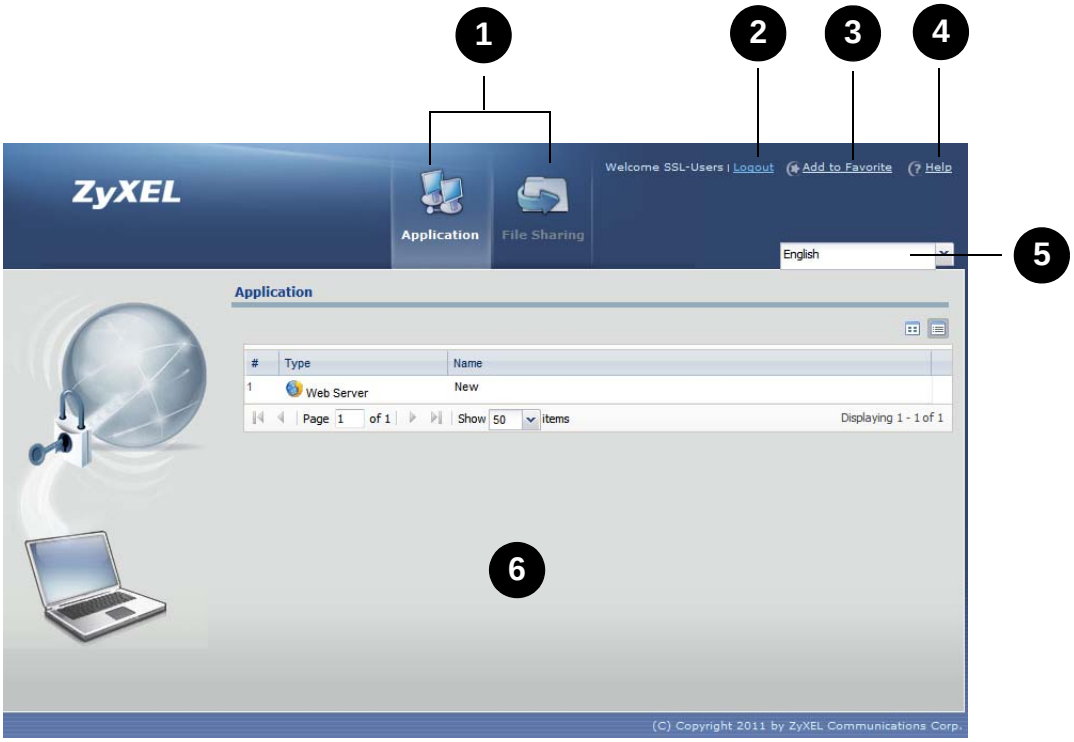
9 The **Application** screen displays showing the list of resources available to you. See Figure 209 on page 332 for a screen example.

Note: Available resource links vary depending on the configuration your network administrator made.

22.3 The SSL VPN User Screens

This section describes the main elements in the remote user screens.

Figure 209 Remote User Screen



The following table describes the various parts of a remote user screen.

Table 120 Remote User Screen Overview

#	DESCRIPTION
1	Click on a menu tab to go to the **Application** or **File Sharing** screen.
2	Click this icon to log out and terminate the secure connection.
3	Click this icon to create a bookmark to the SSL VPN user screen in your web browser.
4	Click this icon to display the on-line help window.
5	Select your preferred language for the interface.
6	This part of the screen displays a list of the resources available to you. In the **Application** screen, click on a link to access or display the access method. In the **File Sharing** screen, click on a link to open a file or directory.

22.4 Bookmarking the ZyWALL

You can create a bookmark of the ZyWALL by clicking the **Add to Favorite** icon. This allows you to access the ZyWALL using the bookmark without having to enter the address every time.

1 In any remote user screen, click the **Add to Favorite** icon.

2 A screen displays. Accept the default name in the **Name** field or enter a descriptive name to identify this link.

3 Click **OK** to create a bookmark in your web browser.

Figure 210 Add Favorite



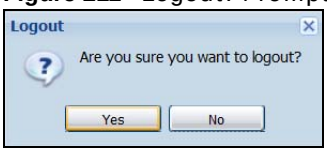
22.5 Logging Out of the SSL VPN User Screens

To properly terminate a connection, click on the **Logout** icon in any remote user screen.

1 Click the **Logout** icon in any remote user screen.

2 A prompt window displays. Click **OK** to continue.

Figure 211 Logout: Prompt



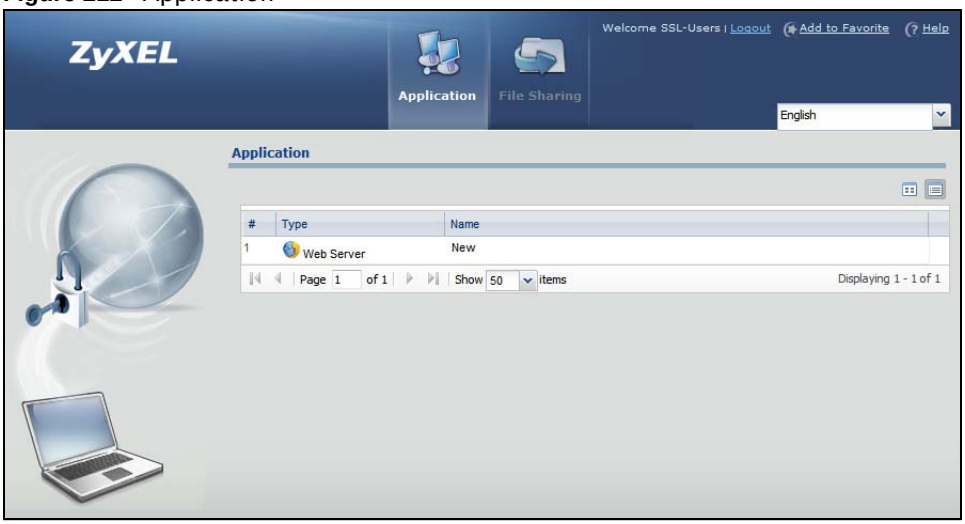
22.6 SSL User Application Screen

Use the **Application** tab's screen to access web-based applications (such as web sites and e-mail) on the network through the SSL VPN connection. Which applications you can access depends on the ZyWALL's configuration.

The **Name** field displays the descriptive name for an application. The **Type** field displays wether the application is a web site (**Web Server**) or web-based e-mail using Microsoft Outlook Web Access (**OWA**).

To access a web-based application, simply click a link in the **Application** screen to display the web screen in a separate browser window.

Figure 212 Application



22.7 SSL User File Sharing

The **File Sharing** screen lets you access files on a file server through the SSL VPN connection. Use it to display and access shared files/folders on a file server.

You can also perform the following actions:

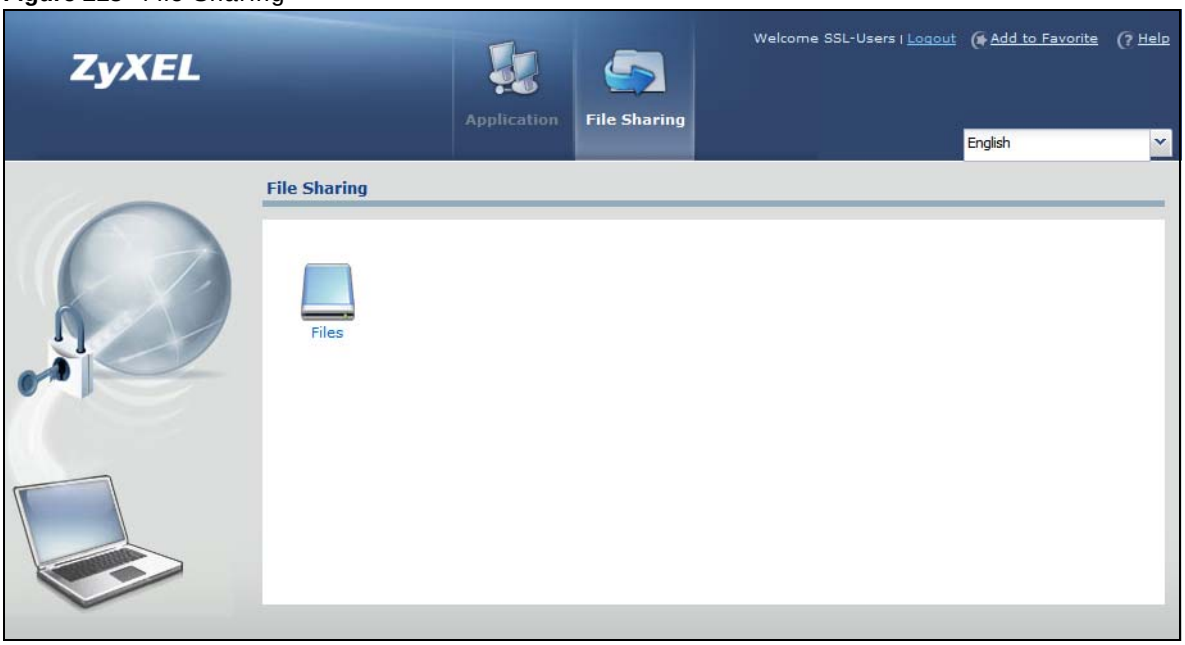
- Access a folder.
- Open a file (if your web browser cannot open the file, you are prompted to download it).
- Save a file to your computer.
- Create a new folder.
- Rename a file or folder.
- Delete a file or folder.
- Upload a file.

Note: Available actions you can perform in the **File Sharing** screen vary depending on the rights granted to you on the file server.

22.7.1 The Main File Sharing Screen

The first **File Sharing** screen displays the name(s) of the shared folder(s) available. The following figure shows an example with one file share.

Figure 213 File Sharing



22.7.2 Opening a File or Folder

You can open a file if the file extension is recognized by the web browser and the associated application is installed on your computer.

1 Log in as a remote user and click the **File Sharing** tab.

2 Click on a file share icon.

3 If an access user name and password are required, a screen displays as shown in the following figure. Enter the account information and click **Login** to continue.

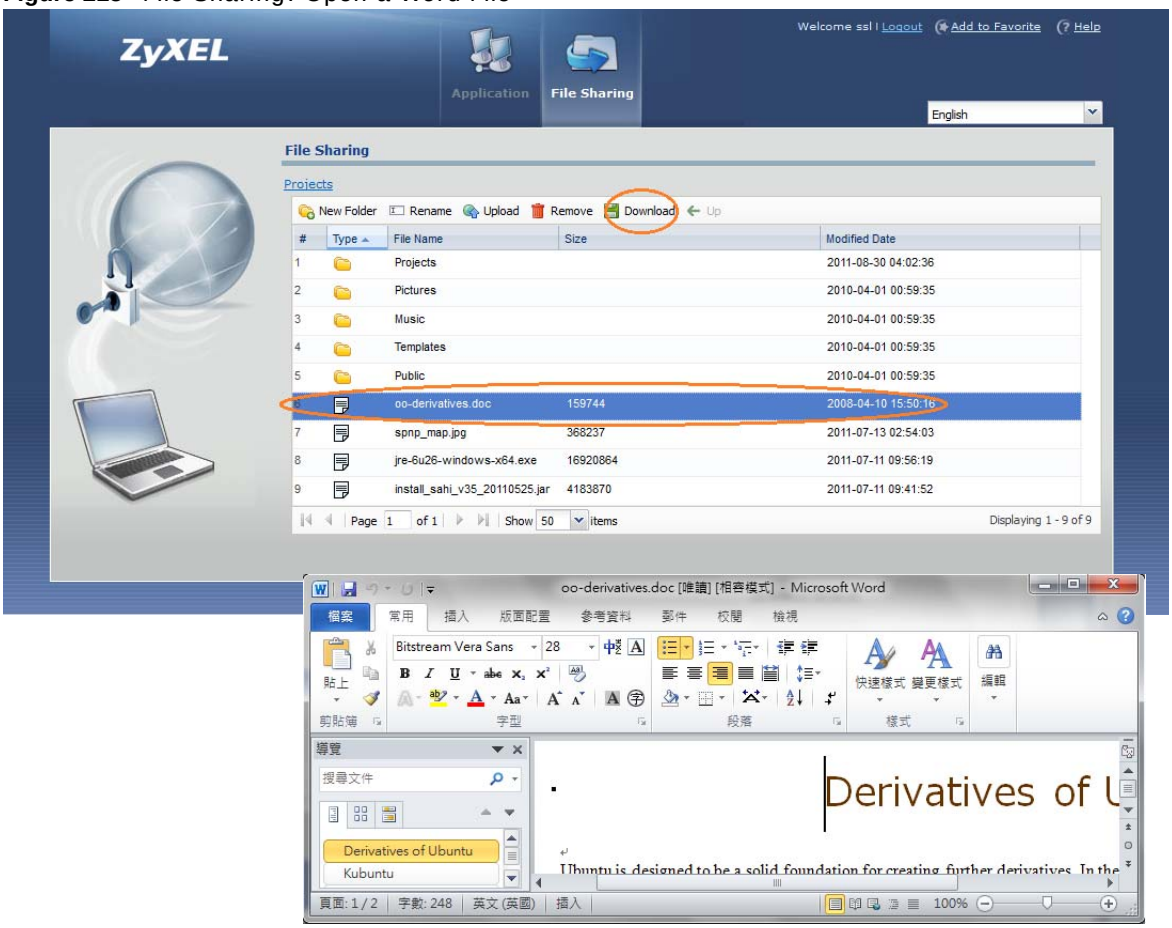
Figure 214 File Sharing: Enter Access User Name and Password



4 A list of files/folders displays. Double click a file to open it in a separate browser window or select a file and click **Download** to save it to your computer. You can also click a folder to access it.

For this example, click on a .doc file to open the Word document.

Figure 215 File Sharing: Open a Word File



22.7.3 Downloading a File

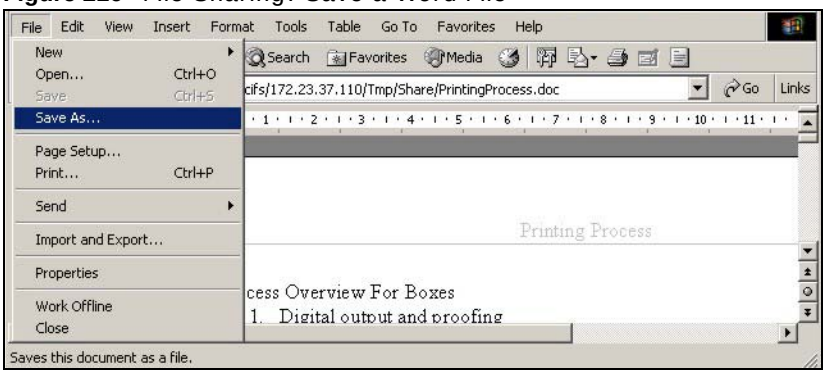
You are prompted to download a file which cannot be opened using a web browser.

Follow the on-screen instructions to download and save the file to your computer. Then launch the associated application to open the file.

22.7.4 Saving a File

After you have opened a file in a web browser, you can save a copy of the file by clicking **File > Save As** and following the on-screen instructions.

Figure 216 File Sharing: Save a Word File



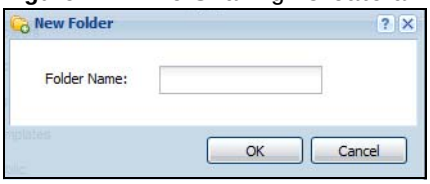
22.7.5 Creating a New Folder

To create a new folder in the file share location, click the **New Folder** icon.

Specify a descriptive name for the folder. You can enter up to 356 characters. Then click **Add**.

Note: Make sure the length of the folder name does not exceed the maximum allowed on the file server.

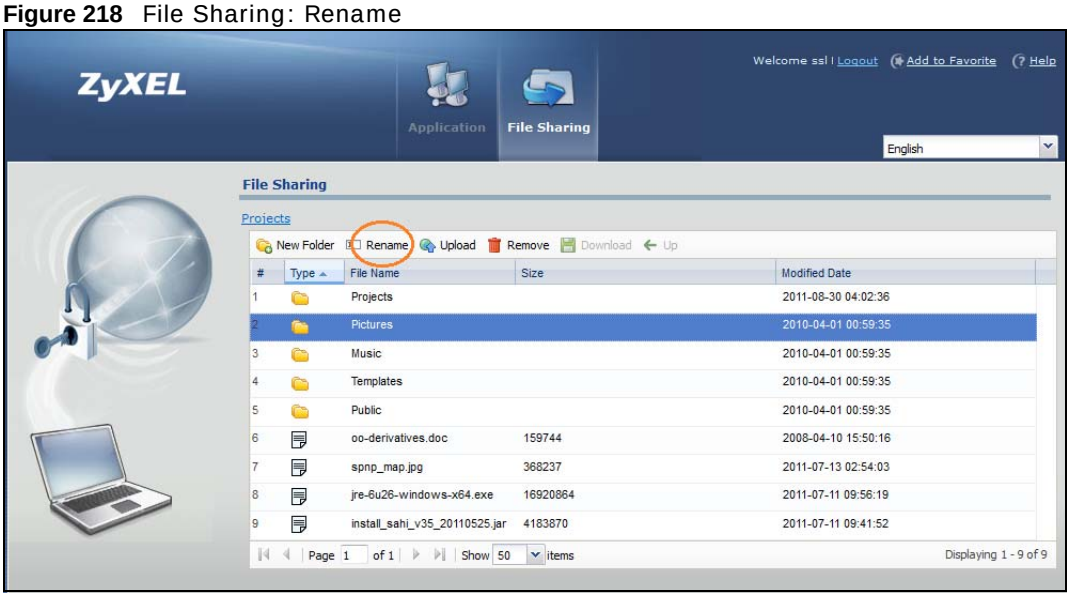
Figure 217 File Sharing: Create a New Folder



22.7.6 Renaming a File or Folder

To rename a file or folder, select a file or folder and click the **Rename** icon.

Figure 218 File Sharing: Rename


ZyXEL
Application
File Sharing
Welcome ssl ! Logout Add to Favorite Help
English
File Sharing
Projects
New Folder Rename Upload Remove Download Up
Type File Name Size Modified Date
1 Projects 2011-08-30 04:02:36
2 Pictures 2010-04-01 00:59:35
3 Music 2010-04-01 00:59:35
4 Templates 2010-04-01 00:59:35
5 Public 2010-04-01 00:59:35
6 oo-derivatives.doc 159744 2008-04-10 15:50:16
7 spnp_map.jpg 368237 2011-07-13 02:54:03
8 jre-6u26-windows-x64.exe 16920864 2011-07-11 09:56:19
9 install_sahi_v35_20110525.jar 4183870 2011-07-11 09:41:52
Page 1 of 1 Show 50 items
Displaying 1 - 9 of 9

A popup window displays. Specify the new name and/or file extension in the field provided. You can enter up to 356 characters. Then click **Apply**.

Note: Make sure the length of the name does not exceed the maximum allowed on the file server.
You may not be able to open a file if you change the file extension.

Figure 219 File Sharing: Rename



22.7.7 Deleting a File or Folder

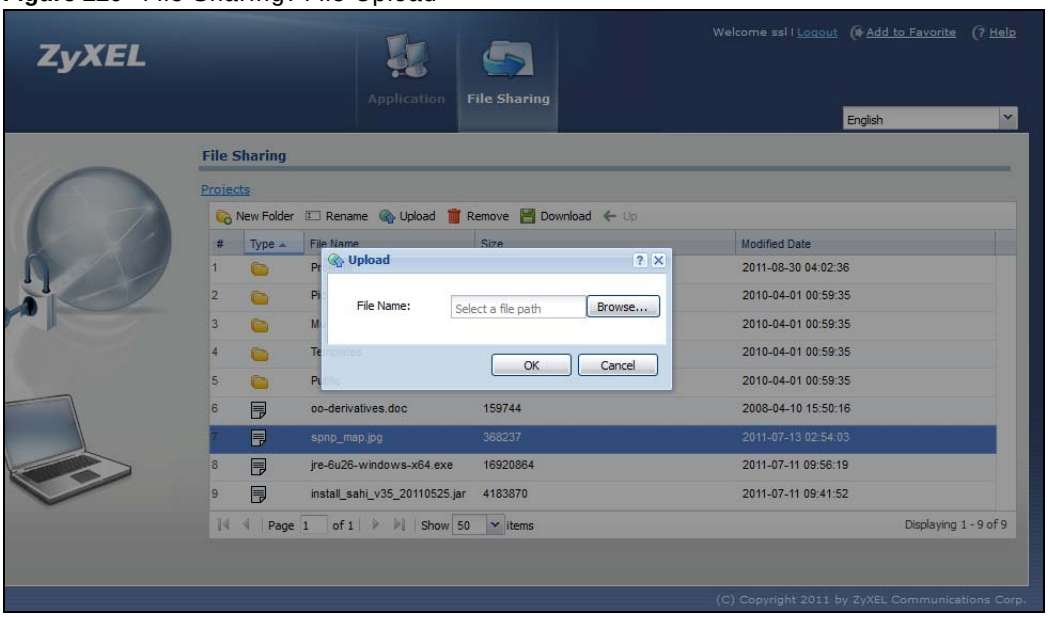
Click the **Delete** icon next to a file or folder to remove it.

22.7.8 Uploading a File

Follow the steps below to upload a file to the file server.

1. Log into the remote user screen and click the **File Sharing** tab.
2. Click **Upload** and specify the location and/or name of the file you want to upload. Or click **Browse** to locate it.
3. Click **OK** to send the file to the file server.
4. After the file is uploaded successfully, you should see the name of the file and a message in the screen.

Figure 220 File Sharing: File Upload



Note: Uploading a file with the same name and file extension replaces the existing file on the file server. No warning message is displayed.

23

ZyWALL SecuExtender

The ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer after a successful login to an SSL VPN tunnel with network extension support enabled. The ZyWALL SecuExtender lets you:

- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the ZyWALL's web-based e-mail.
- Use applications, even proprietary applications, for which the ZyWALL does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer.

23.1 The ZyWALL SecuExtender Icon

The ZyWALL SecuExtender icon color indicates the SSL VPN tunnel's connection status.

Figure 221 ZyWALL SecuExtender Icon

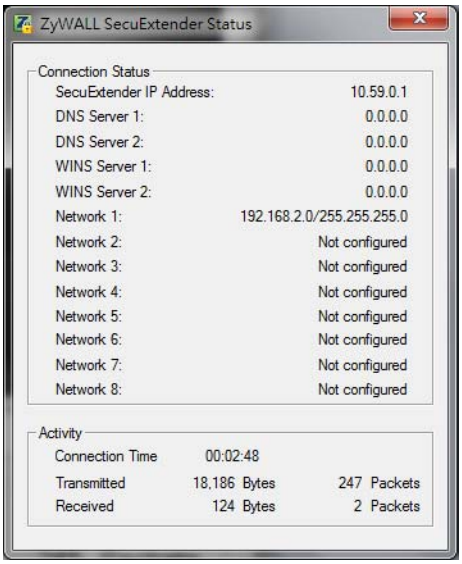


- Green: the SSL VPN tunnel is connected. You can connect to the SSL application and network resources. You can also use another application to access resources behind the ZyWALL.
- Gray: the SSL VPN tunnel's connection is suspended. This means the SSL VPN tunnel is connected, but the ZyWALL SecuExtender will not send any traffic through it until you right-click the icon and resume the connection.
- Red: the SSL VPN tunnel is not connected. You cannot connect to the SSL application and network resources.

23.2 Status

Right-click the ZyWALL SecuExtender icon in the system tray and select **Status** to open the **Status** screen. Use this screen to view the ZyWALL SecuExtender's connection status and activity statistics.

Figure 222 ZyWALL SecuExtender Status



The following table describes the labels in this screen.

Table 121 ZyWALL SecuExtender Status

LABEL	DESCRIPTION
Connection Status	
SecuExtender IP Address	This is the IP address the ZyWALL assigned to this remote user computer for an SSL VPN connection.
DNS Server 1/2	These are the IP addresses of the DNS server and backup DNS server for the SSL VPN connection. DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Your computer uses the DNS server specified here to resolve domain names for resources you access through the SSL VPN connection.
WINS Server 1/2	These are the IP addresses of the WINS (Windows Internet Naming Service) and backup WINS servers for the SSL VPN connection. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Network 1~8	These are the networks (including netmask) that you can access through the SSL VPN connection.
Activity	
Connected Time	This is how long the computer has been connected to the SSL VPN tunnel.
Transmitted	This is how many bytes and packets the computer has sent through the SSL VPN connection.
Received	This is how many bytes and packets the computer has received through the SSL VPN connection.

23.3 View Log

If you have problems with the ZyWALL SecuExtender, customer support may request you to provide information from the log. Right-click the ZyWALL SecuExtender icon in the system tray and select **Log** to open a notepad file of the ZyWALL SecuExtender's log.

Figure 223 ZyWALL SecuExtender Log Example

```
################################################################################
##############
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Build Datetime: Feb 24 2009/
10:25:07
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]  rasphone.pbk: C:\Documents and
Settings\11746\rasphone.pbk
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]  SecuExtender.log:
C:\Documents and Settings\11746\SecuExtender.log
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Check Parameters
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Connect to 172.23.31.19:443/
10444
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Parameter is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking System status...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking service (first) ...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  SecuExtender Helper is running
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  System is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]  Connect to 2887196435/443
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Handshake LoopCounter: 0
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  611 bytes of handshake data
received
```

23.4 Suspend and Resume the Connection

When the ZyWALL SecuExtender icon in the system tray is green, you can right-click the icon and select **Suspend Connection** to keep the SSL VPN tunnel connected but not send any traffic through it until you right-click the icon and resume the connection.

23.5 Stop the Connection

Right-click the icon and select **Stop Connection** to disconnect the SSL VPN tunnel.

23.6 Uninstalling the ZyWALL SecuExtender

Do the following if you need to remove the ZyWALL SecuExtender.

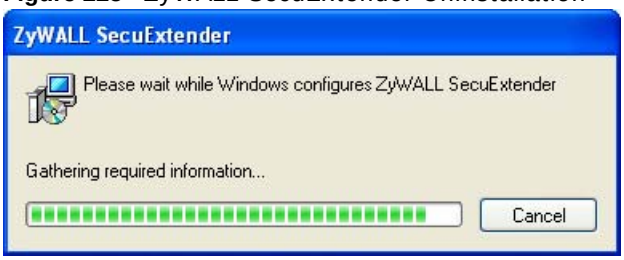
1. Click **start > All Programs > ZyXEL > ZyWALL SecuExtender > Uninstall ZyWALL SecuExtender**.
2. In the confirmation screen, click **Yes**.

Figure 224 Uninstalling the ZyWALL SecuExtender Confirmation



3 Windows uninstalls the ZyWALL SecuExtender.

Figure 225 ZyWALL SecuExtender Uninstallation



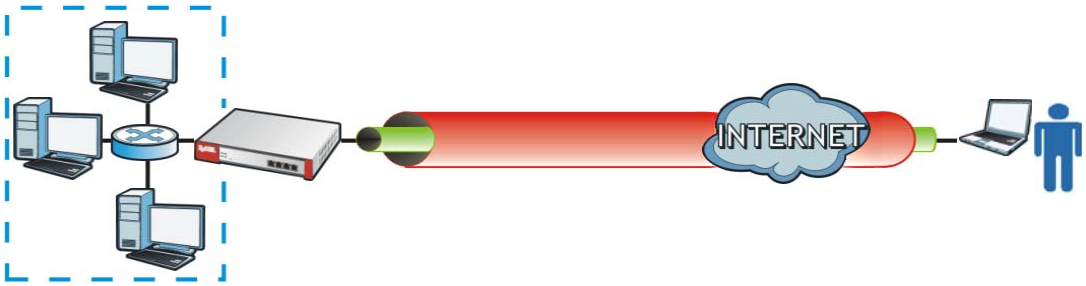
24

L2TP VPN

24.1 Overview

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the ZyWALL. The remote users do not need their own IPSec gateways or third-party VPN client software.

Figure 226 L2TP VPN Overview



24.1.1 What You Can Do in this Chapter

- Use the **L2TP VPN** screen (see Section 24.2 on page 347) to configure the ZyWALL's L2TP VPN settings.

24.1.2 What You Need to Know

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it. See Chapter 20 on page 281 for information on IPSec VPN.

IPSec Configuration Required for L2TP VPN

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 20 on page 281 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Not be a manual key VPN connection.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

Using the Default L2TP VPN Connection

The **Default_L2TP_VPN_GW** gateway entry is pre-configured to be convenient to use for L2TP VPN. Edit it as follows:

- Set **My Address** to the WAN interface domain name or IP address you want to use.
- Replace the default **Pre-Shared Key**.

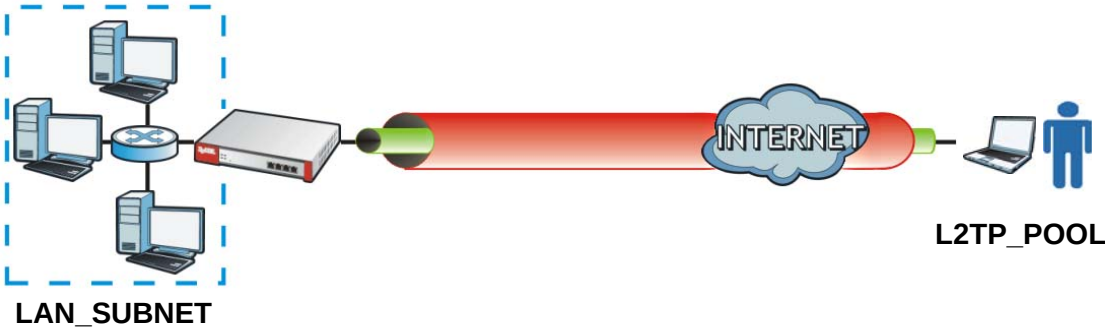
Create a host-type address object containing the **My Address** IP address configured in the **Default_L2TP_VPN_GW** and set the **Default_L2TP_VPN_Connection**'s **Local Policy** to use it.

Policy Route

Configure a policy route to let remote users access resources on a network behind the ZyWALL.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in the following figure).
- Set the **Destination Address** to the IP address pool that the ZyWALL assigns to the remote users (**L2TP_POOL** in the following figure).
- Set the next hop to be the VPN tunnel that you are using for L2TP.

Figure 227 Policy Route for L2TP VPN



To manage the ZyWALL through the L2TP VPN tunnel, create a routing policy that sends the ZyWALL's return traffic back through the L2TP VPN tunnel.

- Set **Incoming** to **ZyWALL.**
- Set **Destination Address** to the L2TP address pool.
- Set the next hop to be the VPN tunnel that you are using for L2TP.

If some of the traffic from the L2TP clients needs to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk.

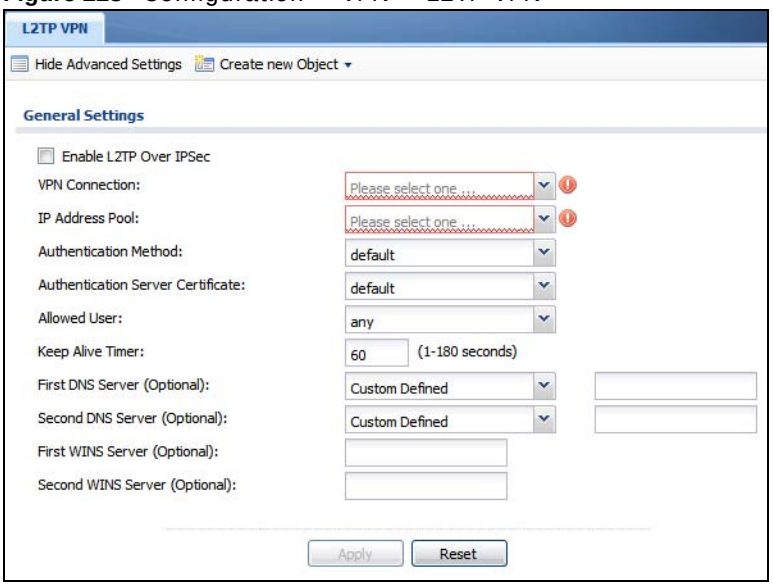
- Set **Incoming** to **Tunnel** and select your L2TP VPN connection.
- Set the **Source Address** to the L2TP address pool.
- Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

24.2 L2TP VPN Screen

Click **Configuration > VPN > L2TP VPN** to open the following screen. Use this screen to configure the ZyWALL's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Figure 228 Configuration > VPN > L2TP VPN



The following table describes the fields in this screen.

Table 122 Configuration > VPN > L2TP VPN

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable L2TP Over IPSec	Use this field to turn the ZyWALL's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the ZyWALL uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in IPSec Configuration Required for L2TP VPN on page 345. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the ZyWALL uses to assign to the L2TP VPN clients. Use **Create new Object** if you need to configure a new pool of IP addresses.
Authentication Method	Select how the ZyWALL authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the ZyWALL check a user's user name and password against the ZyWALL's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these. See Chapter 32 on page 409 for how to create authentication method objects.

Table 122 Configuration > VPN > L2TP VPN (continued)

LABEL	DESCRIPTION
Authentication Server Certificate	Select the certificate to use to identify the ZyWALL for L2TP VPN connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 33 on page 413 for details). The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols.
Allowed User	The remote user must log into the ZyWALL to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Use **Create new Object** if you need to configure a new user account. Otherwise, select **any** to allow any user with a valid account and password on the ZyWALL to log in.
Keep Alive Timer	The ZyWALL sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL disconnects the VPN tunnel if the remote user does not respond.
First DNS Server, Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address. **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click **Apply** to save your changes in the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

25

Bandwidth Management

25.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

25.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see Section 25.2 on page 353) to control bandwidth for services passing through the ZyWALL, and it identifies the conditions that refine this.

25.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over policy routes to manage the bandwidth of TCP and UDP traffic.

If you want to use a service, make sure both the firewall allow the service's packets to go through the ZyWALL.

Note: The ZyWALL checks firewall rules before it checks bandwidth management rules for traffic going through the ZyWALL.

Bandwidth management examines every TCP and UDP connection passing through the ZyWALL. Then, you can specify, by port, whether or not the ZyWALL continues to route the connection.

DiffServ and DSCP Marking

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is from which interface the connection was initiated and to which interface the connection is going.

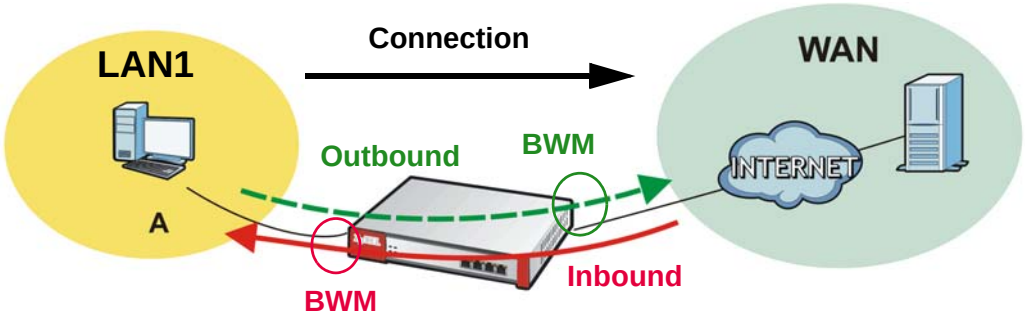
A connection has outbound and inbound packet flows. The ZyWALL controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the ZyWALL.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 229 LAN1 to WAN Connection and Packet Directions

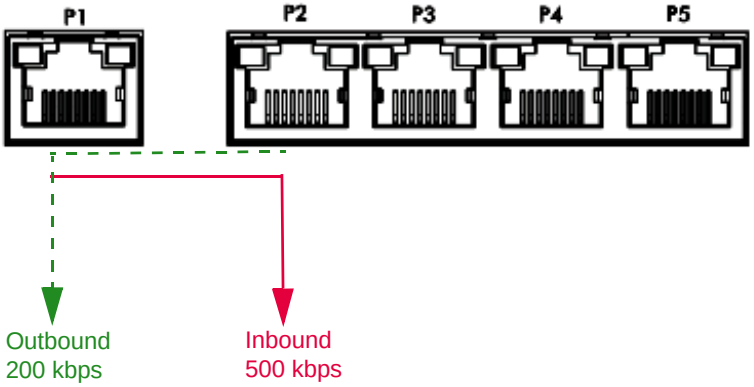


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 230 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The ZyWALL gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The ZyWALL automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

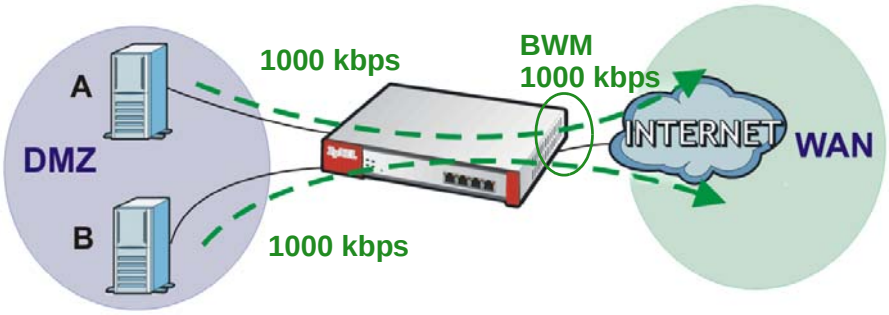
After each application gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**’s traffic and policy B for server **B**’s traffic.

Figure 231 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 123 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server **B**.

Table 124 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the ZyWALL divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 125 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the ZyWALL still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 126 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

Finding Out More

- See DSCP Marking and Per-Hop Behavior on page 189 for a description of DSCP marking.

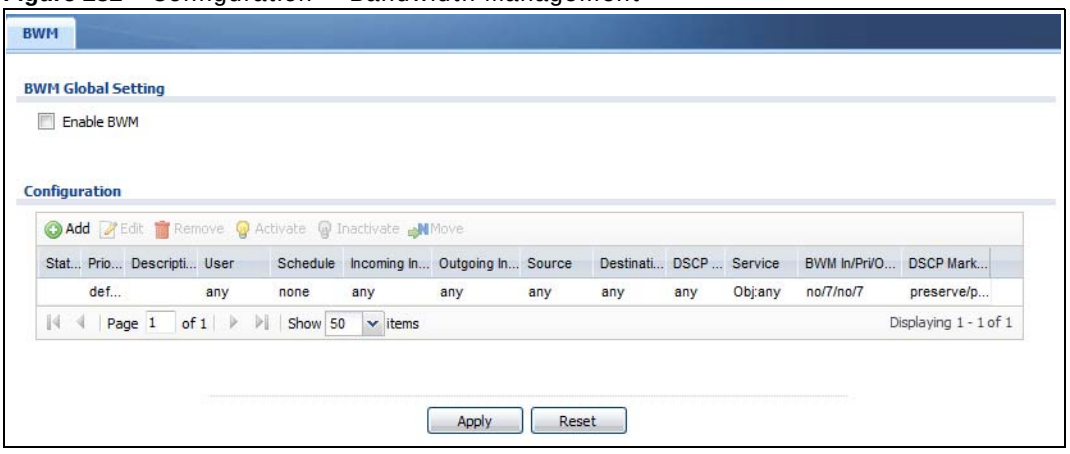
25.2 The Bandwidth Management Screen

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify how the ZyWALL handles the DSCP value and allocate bandwidth for the matching packets.

Click **Configuration > BWM** to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of “default”. It is the last policy the ZyWALL checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 232 Configuration > Bandwidth Management



The following table describes the labels in this screen. See Section 25.2.1 on page 355 for more information as well.

Table 127 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This field displays a sequential value for each bandwidth management policy and it is not associated with a specific setting. This field displays **default** for the default bandwidth management policy.
Description	This field displays additional information about this policy.
User	This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users.
Schedule	This is the schedule that defines when the policy applies. **none** means the policy always applies.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination.
DSCP Code	These are the DSCP code point values of incoming and outgoing packets to which this policy applies. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" options stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Section 10.4 on page 208 for more details.
Service Type	**App** and the service name displays if you selected **App Patrol Service** for the service type. An **App Patrol Service** is a pre-defined service. **Obj** and the service name displays if you selected **Service Object** for the service type. A **Service Object** is a customized pre-defined service or another service. Mouse over the service object name to view the corresponding IP protocol number.

Table 127 Configuration > Bandwidth Management

LABEL	DESCRIPTION
BWM In/Pri/Out/Pri	This field shows the amount of bandwidth the traffic can use. **In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the inbound traffic. **Out** - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the outbound traffic. **Pri** - This is the priority for the incoming (the first **Pri** value) or outgoing (the second **Pri** value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ZyWALL ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
DSCP Marking	This is how the ZyWALL handles the DSCP value of the incoming and outgoing packets that match this policy. **In** - Inbound, the traffic the ZyWALL sends to a connection's initiator. **Out** - Outbound, the traffic the ZyWALL sends out from a connection's initiator. If this field displays a DSCP value, the ZyWALL applies that DSCP value to the route's outgoing packets. **preserve** means the ZyWALL does not modify the DSCP value of the route's outgoing packets. **default** means the ZyWALL sets the DSCP value of the route's outgoing packets to 0. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Section 10.4 on page 208 for more details.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

25.2.1 The Bandwidth Management Add/Edit Screen

The **Configuration > Bandwidth Management Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Configuration > Bandwidth Management** screen (see Section 25.2 on page 353), and click either the **Add** icon or an **Edit** icon.

Figure 233 Configuration > Bandwidth Management > Edit (For the Default Policy)

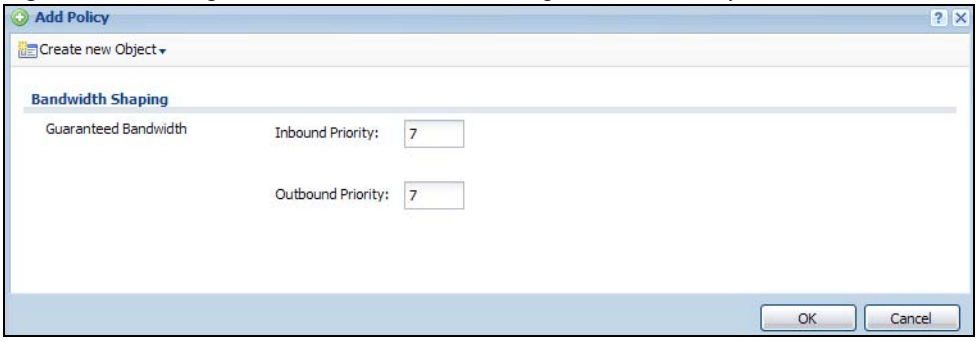
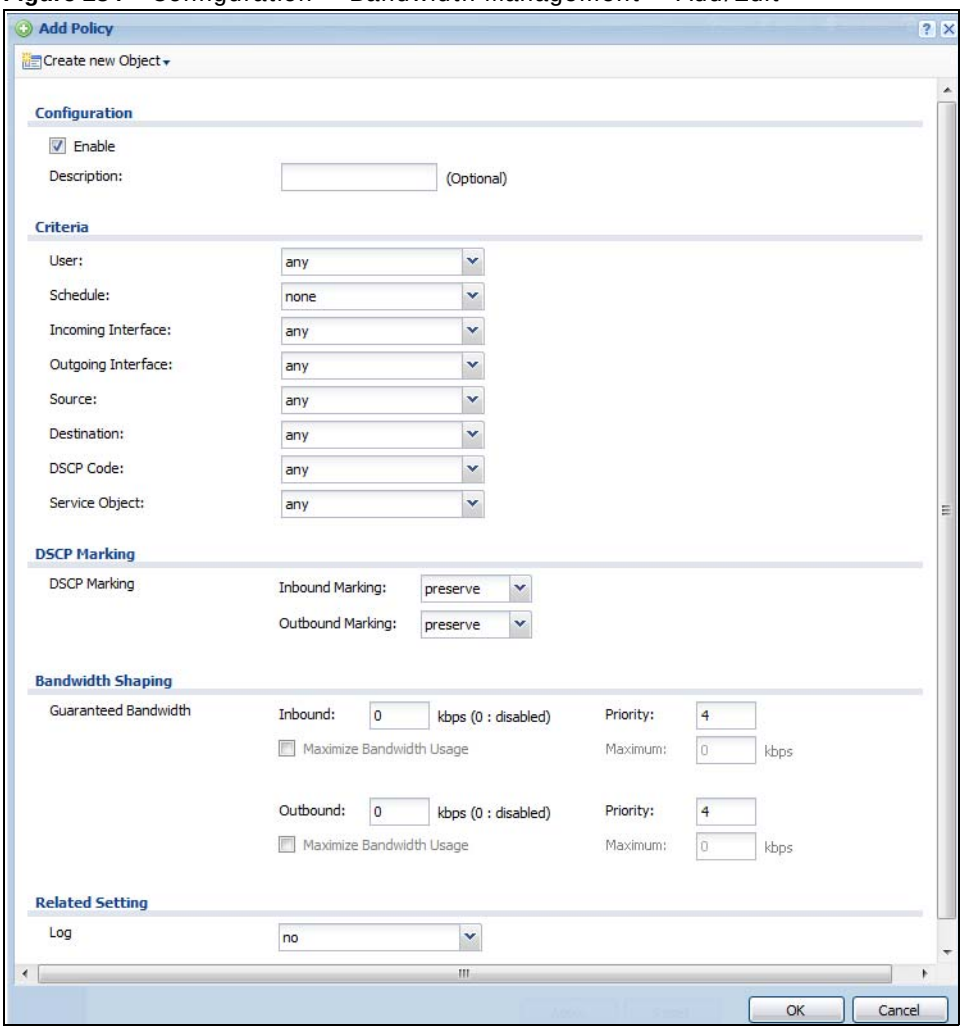


Figure 234 Configuration > Bandwidth Management > Add/Edit



The following table describes the labels in this screen.

Table 128 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this check box to turn on this policy.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.
User	Select a user name or user group to which to apply the policy. Use **Create new Object** if you need to configure a new user account. Select **any** to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 30 on page 396 for details). Otherwise, select **none** to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.

Table 128 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select **User Defined** to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Section 10.4 on page 208 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service	This field is available if you selected **Service Object** as the service type. Select a service or service group to identify the type of traffic to which this policy applies. **any** means all services.
DSCP Marking	Set how the ZyWALL handles the DSCP value of the incoming and outgoing packets that match this policy. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select **User Defined** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Section 10.4 on page 208 for more details. Select **preserve** to have the ZyWALL keep the packets' original DSCP value. Select **default** to have the ZyWALL set the DSCP value of the packets to 0.
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

Table 128 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	This field displays when the inbound or outbound bandwidth management is not set to 0. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.
Related Setting	
Log	Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when any traffic matches this policy. See Chapter 38 on page 485 for more on logs.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

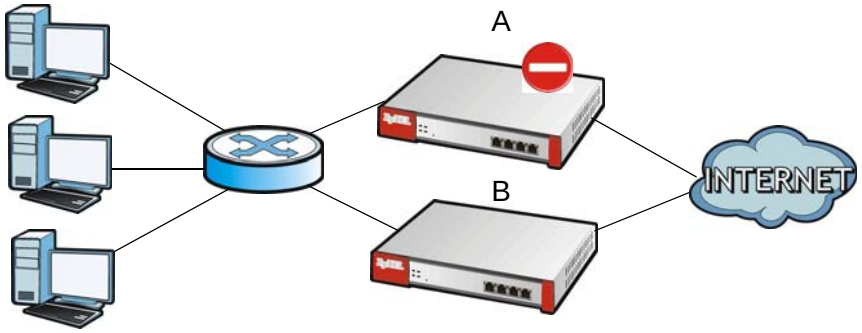
26

Device HA

26.1 Overview

Device HA lets a backup ZyWALL (**B**) automatically take over if the master ZyWALL (**A**) fails.

Figure 235 Device HA Backup Taking Over for the Master



26.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 26.2 on page 360) to configure device HA global settings, and see the status of each interface monitored by device HA.
- Use the **Active-Passive Mode** screens (Section 26.3 on page 361) to use active-passive mode device HA. You can configure general active-passive mode device HA settings, view and manage the list of monitored interfaces, and synchronize backup ZyWALLs.

26.1.2 What You Need to Know

Active-Passive Mode

- Active-passive mode lets a backup ZyWALL take over if the master ZyWALL fails.

Management Access

You can configure a separate management IP address for each interface. You can use it to access the ZyWALL for management whether the ZyWALL is the master or a backup. The management IP address should be in the same subnet as the interface IP address.

Synchronization

Use synchronization to have a backup ZyWALL copy the master ZyWALL's configuration, and certificates.

Note: Only ZyWALLs of the same model and firmware version can synchronize.

Otherwise you must manually configure the master ZyWALL's settings on the backup (by editing copies of the configuration files in a text editor for example).

Finding Out More

- See Section 26.5 on page 366 for device HA background/technical information.

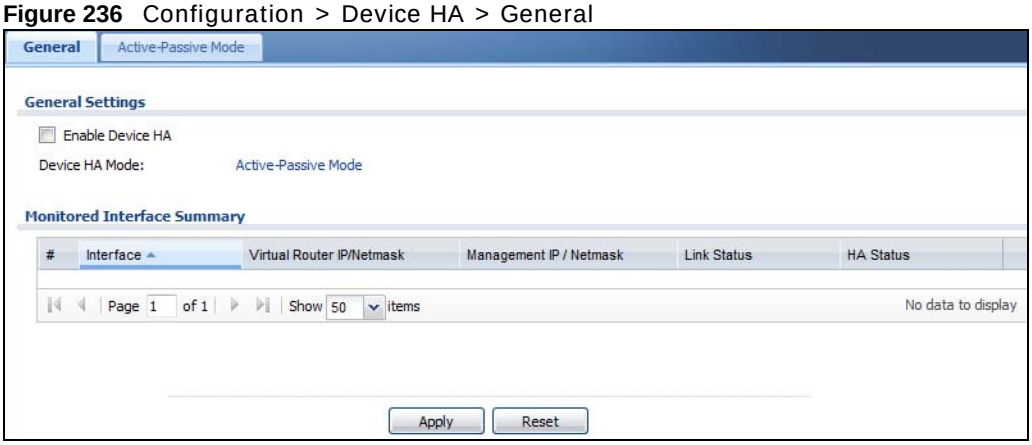
26.1.3 Before You Begin

- Configure a static IP address for each interface that you will have device HA monitor.

26.2 Device HA General

The **Configuration > Device HA General** screen lets you enable or disable device HA, and displays which device HA mode the ZyWALL is set to use along with a summary of the monitored interfaces.

Figure 236 Configuration > Device HA > General



The following table describes the labels in this screen.

Table 129 Configuration > Device HA > General

LABEL	DESCRIPTION
Enable Device HA	Turn the ZyWALL's device HA feature on or off. Note: It is not recommended to use STP (Spanning Tree Protocol) with device HA.
Device HA Mode	This displays the ZyWALL is currently set to use active-passive mode device HA.
Monitored Interface Summary	This table shows the status of the interfaces that you selected for monitoring in the other device HA screens.
#	This is the entry's index number in the list.
Interface	These are the names of the interfaces that are monitored by device HA.
Virtual Router IP / Netmask	This is the interface's IP address and subnet mask. Whichever ZyWALL is the master uses this virtual router IP address and subnet mask.

Table 129 Configuration > Device HA > General (continued)

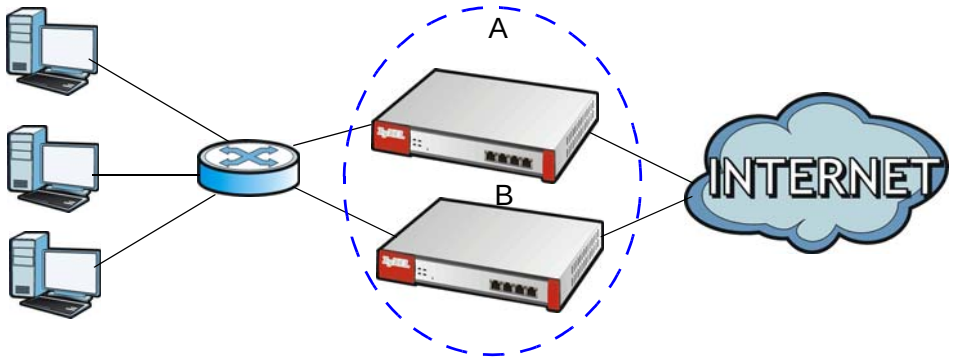
LABEL	DESCRIPTION
Management IP / Netmask	This field displays the interface's management IP address and subnet mask. You can use this IP address and subnet mask to access the ZyWALL whether it is in master or backup mode.
Link Status	This tells whether the monitored interface's connection is down or up.
HA Status	The text before the slash shows whether the device is configured as the master or the backup role. This text after the slash displays the monitored interface's status in the virtual router. **Active** - This interface is up and using the virtual IP address and subnet mask. **Stand-By** - This interface is a backup interface in the virtual router. It is not using the virtual IP address and subnet mask. **Fault** - This interface is not functioning in the virtual router right now. In active-passive mode , if one of the master ZyWALL's interfaces loses its connection, the master ZyWALL forces all of its interfaces to the fault state so the backup ZyWALL can take over all of the master ZyWALL's functions.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

26.3 The Active-Passive Mode Screen

Virtual Router

The master and backup ZyWALL form a single 'virtual router'. In the following example, master ZyWALL **A** and backup ZyWALL **B** form a virtual router.

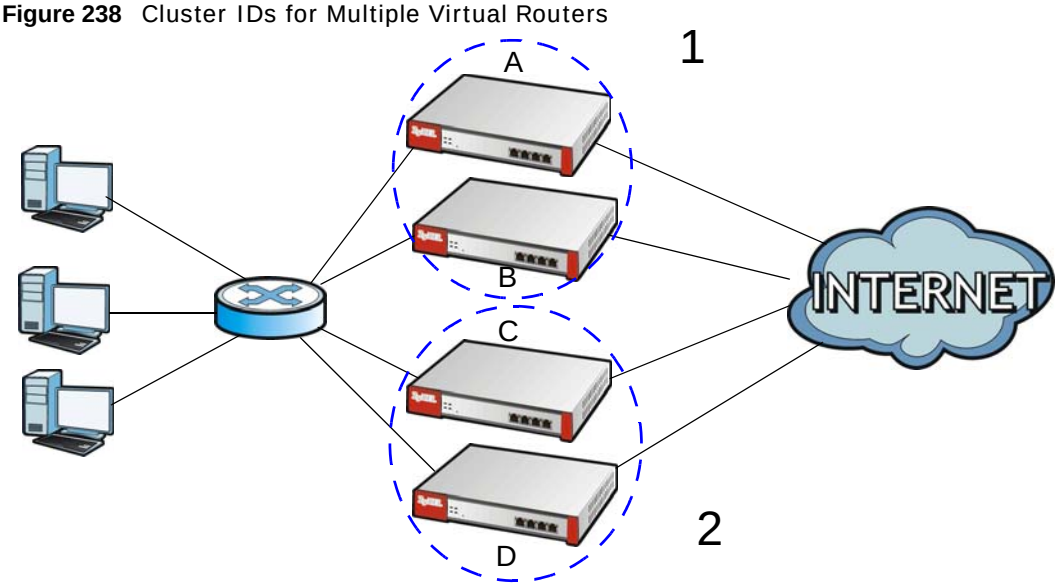
Figure 237 Virtual Router



Cluster ID

You can have multiple ZyWALL virtual routers on your network. Use a different cluster ID to identify each virtual router. In the following example, ZyWALLs **A** and **B** form a virtual router that uses cluster ID 1. ZyWALLs **C** and **D** form a virtual router that uses cluster ID 2.

Figure 238 Cluster IDs for Multiple Virtual Routers



Monitored Interfaces in Active-Passive Mode Device HA

You can select which interfaces device HA monitors. If a monitored interface on the ZyWALL loses its connection, device HA has the backup ZyWALL take over.

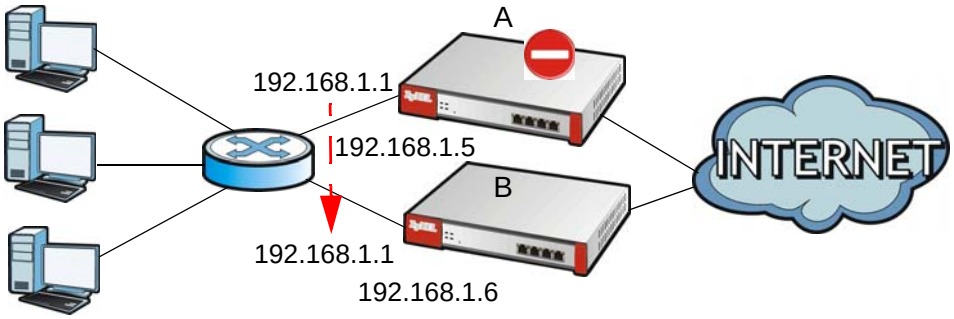
Enable monitoring for the same interfaces on the master and backup ZyWALLs. Each monitored interface must have a static IP address and be connected to the same subnet as the corresponding interface on the backup or master ZyWALL.

Virtual Router and Management IP Addresses

- If a backup takes over for the master, it uses the master's IP addresses. These IP addresses are know as the virtual router IP addresses.
- Each interface can also have a management IP address. You can connect to this IP address to manage the ZyWALL regardless of whether it is the master or the backup.

For example, ZyWALL **B** takes over **A**'s 192.168.1.1 LAN interface IP address. This is a virtual router IP address. ZyWALL **A** keeps it's LAN management IP address of 192.168.1.5 and ZyWALL **B** has its own LAN management IP address of 192.168.1.6. These do not change when ZyWALL **B** becomes the master.

Figure 239 Management IP Addresses



26.3.1 Configuring Active-Passive Mode Device HA

The **Device HA Active-Passive Mode** screen lets you configure general active-passive mode device HA settings, view and manage the list of monitored interfaces, and synchronize backup ZyWALLs. To access this screen, click **Configuration > Device HA > Active-Passive Mode**.

The following table describes the labels in this screen. See Section 26.4 on page 365 for more information as well.

Table 130 Configuration > Device HA > Active-Passive Mode

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Device Role	Select the device HA role that the ZyWALL plays in the virtual router. Choices are: **Master** - This ZyWALL is the master ZyWALL in the virtual router. This ZyWALL uses the virtual IP address for each monitored interface. Note: Do not set this field to **Master** for two or more ZyWALLs in the same virtual router (same cluster ID). **Backup** - This ZyWALL is a backup ZyWALL in the virtual router. This ZyWALL does not use any of the virtual IP addresses.
Priority	This field is available for a backup ZyWALL. Type the priority of the backup ZyWALL. The backup ZyWALL with the highest value takes over the role of the master ZyWALL if the master ZyWALL becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
Enable Preemption	This field is available for a backup ZyWALL. Select this if this ZyWALL should become the master ZyWALL if a lower-priority ZyWALL is the master when this one is enabled. (If the role is master, the ZyWALL preempts by default.)
Cluster Settings	
Cluster ID	Type the cluster ID number. A virtual router consists of a master ZyWALL and all of its backup ZyWALLs. If you have multiple ZyWALL virtual routers on your network, use a different cluster ID for each virtual router.
Authentication	Select the authentication method the virtual router uses. Every interface in a virtual router must use the same authentication method and password. Choices are: **None** - this virtual router does not use any authentication method. **Text** - this virtual router uses a plain text password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long. **IP AH (MD5)** - this virtual router uses an encrypted MD5 password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long. See Authentication Types on page 209 for more information about authentication methods.
Monitored Interface Summary	This table shows the status of the device HA settings and status of the ZyWALL’s interfaces.
Edit	Select an entry and click this to be able to modify it.
Activate	To turn on an entry, select it and click **Activate**.

Table 130 Configuration > Device HA > Active-Passive Mode (continued)

LABEL	DESCRIPTION
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This field identifies the interface. At the time of writing, Ethernet and bridge interfaces can be included in the active-passive mode virtual router. The member interfaces of any bridge interfaces do not display separately.
Virtual Router IP / Netmask	This is the master ZyWALL's (static) IP address and subnet mask for this interface. If a backup takes over for the master, it uses this IP address. These fields are blank if the interface is a DHCP client or has no IP settings.
Management IP / Netmask	This field displays the interface's management IP address and subnet mask. You can use this IP address and subnet mask to access the ZyWALL whether it is in master or backup mode.
Link Status	This tells whether the monitored interface's connection is down or up.
Synchronization	Use synchronization to have a backup ZyWALL copy the master ZyWALL's configuration, certificates. Every interface's management IP address must be in the same subnet as the interface's IP address (the virtual router IP address).
Server Address	If this ZyWALL is set to backup role, enter the IP address or Fully-Qualified Domain Name (FQDN) of the ZyWALL from which to get updated configuration. Usually, you should enter the IP address or FQDN of a virtual router on a secure network. If this ZyWALL is set to master role, this field displays the ZyWALL's IP addresses and/or Fully-Qualified Domain Names (FQDN) through which ZyWALLs in backup role can get updated configuration from this ZyWALL.
Sync. Now	This displays if the ZyWALL is set to use active-passive mode device HA, the ZyWALL is in the backup role and device HA is enabled. Click this to copy the specified ZyWALL's configuration.
Server Port	If this ZyWALL is set to the backup role, enter the port number to use for Secure FTP when synchronizing with the specified master ZyWALL. If this ZyWALL is set to master role, this field displays the ZyWALL's Secure FTP port number. Click the **Configure** link if you need to change the FTP port number. Every ZyWALL in the virtual router must use the same port number. If the master ZyWALL changes, you have to manually change this port number in the backups.
Password	Enter the password used for verification during synchronization. Every ZyWALL in the virtual router must use the same password. If you leave this field blank in the master ZyWALL, no backup ZyWALLs can synchronize from it. If you leave this field blank in a backup ZyWALL, it cannot synchronize from the master ZyWALL.
Retype to Confirm	Type the password again here to confirm it.
Auto Synchronize	Select this to get the updated configuration automatically from the specified ZyWALL according to the specified **Interval**. The first synchronization begins after the specified **Interval**; the ZyWALL does not synchronize immediately.
Interval	When you select **Auto Synchronize**, set how often the ZyWALL synchronizes with the master.
Next Sync Time	This appears the next time and date (in hh:mm yyyy-mm-dd format) the ZyWALL will synchronize with the master.

Table 130 Configuration > Device HA > Active-Passive Mode (continued)

LABEL	DESCRIPTION
Apply	This appears when the ZyWALL is currently using active-passive mode device HA. Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

26.4 Configuring an Active-Passive Mode Monitored Interface

The **Device HA Active-Passive Mode Monitored Interface Edit** screen lets you enable or disable monitoring of an interface and set the interface's management IP address and subnet mask. To access this screen, click **Configuration > Device HA > Active-Passive Mode > Edit**.

If you configure device HA settings for an Ethernet interface and later add the Ethernet interface to a bridge, the ZyWALL retains the interface's device HA settings and uses them again if you later remove the interface from the bridge. If the bridge is later deleted or the interface is removed from it, Device HA will recover the interface's setting.

A bridge interface's device HA settings are not retained if you delete the bridge interface.

Figure 240 Configuration > Device HA > Active-Passive Mode > Edit

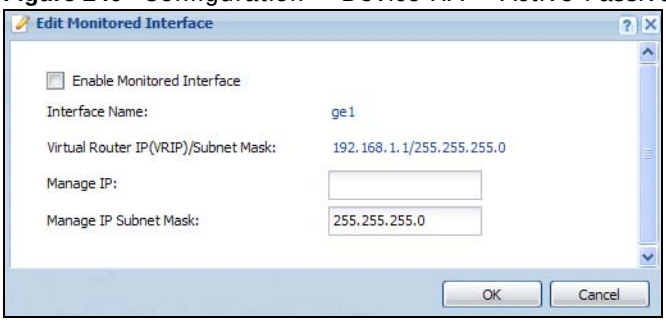
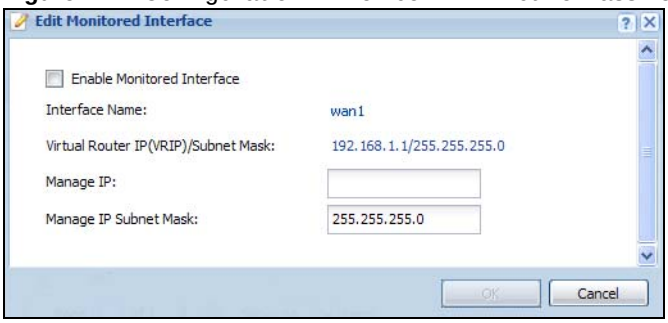


Figure 241 Configuration > Device HA > Active-Passive Mode > Edit



The following table describes the labels in this screen.

Table 131 Configuration > Device HA > Active-Passive Mode > Edit

LABEL	DESCRIPTION
Enable Monitored Interface	Select this to have device HA monitor the status of this interface's connection.
Interface Name	This identifies the interface. Note: Do not connect the bridge interfaces on two ZyWALLs without device HA activated on both. Doing so could cause a broadcast storm. Either activate device HA before connecting the bridge interfaces or disable the bridge interfaces, connect the bridge interfaces, activate device HA, and finally reactivate the bridge interfaces.
Virtual Router IP (VRIP) / Subnet Mask	This is the interface's (static) IP address and subnet mask in the virtual router. Whichever ZyWALL is currently serving as the master uses this virtual router IP address and subnet mask. These fields are blank if the interface is a DHCP client or has no IP settings.
Manage IP	Enter the interface's IP address for management access. You can use this IP address to access the ZyWALL whether it is the master or a backup. This management IP address should be in the same subnet as the interface IP address.
Manage IP Subnet Mask	Enter the subnet mask of the interface's management IP address.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

26.5 Device HA Technical Reference

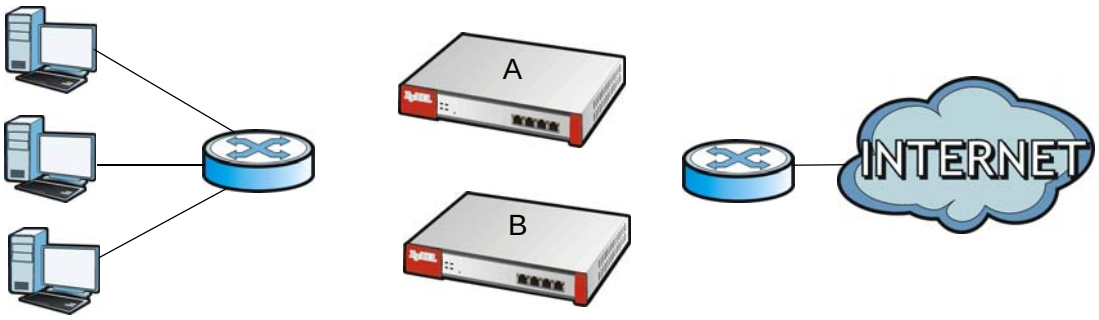
Active-Passive Mode Device HA with Bridge Interfaces

Here are two ways to avoid a broadcast storm when you connect the bridge interfaces on two ZyWALLs.

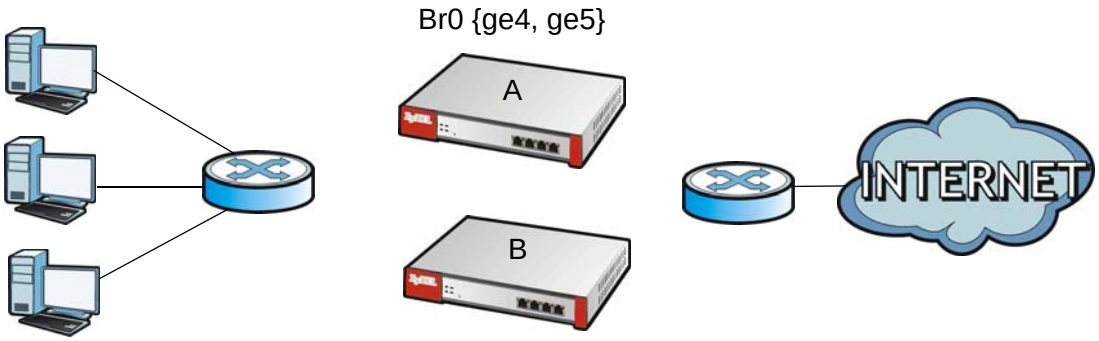
First Option for Connecting the Bridge Interfaces on Two ZyWALLs

The first way is to activate device HA before connecting the bridge interfaces as shown in the following example.

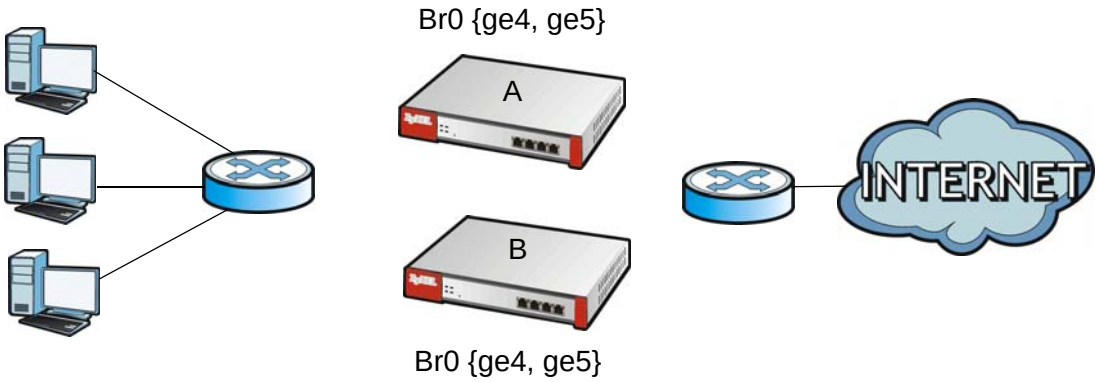
1 Make sure the bridge interfaces of the master ZyWALL (**A**) and the backup ZyWALL (**B**) are not connected.



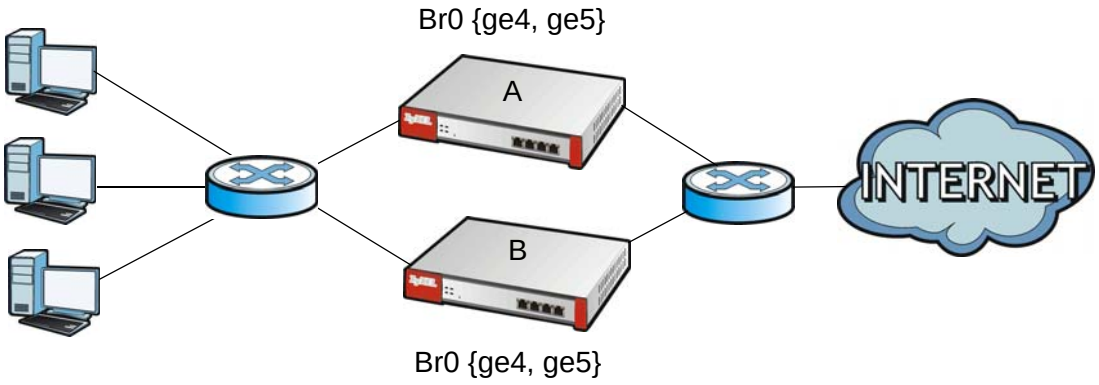
2 Configure the bridge interface on the master ZyWALL, set the bridge interface as a monitored interface, and activate device HA.



3 Configure the bridge interface on the backup ZyWALL, set the bridge interface as a monitored interface, and activate device HA.



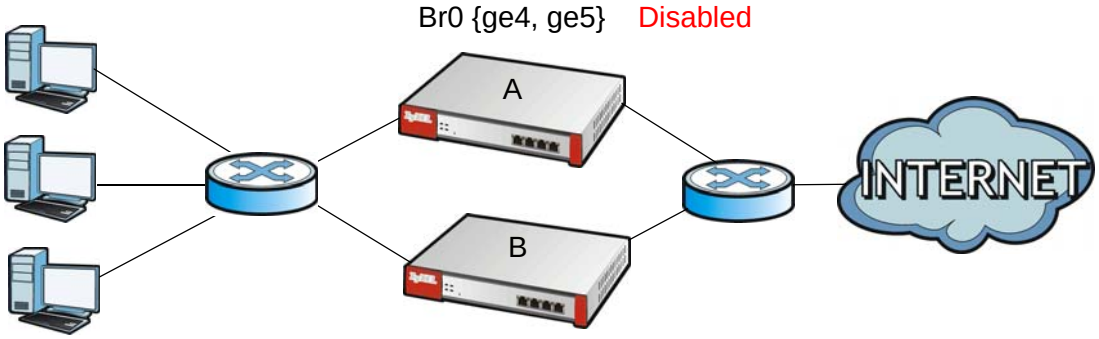
4 Connect the ZyWALLs.



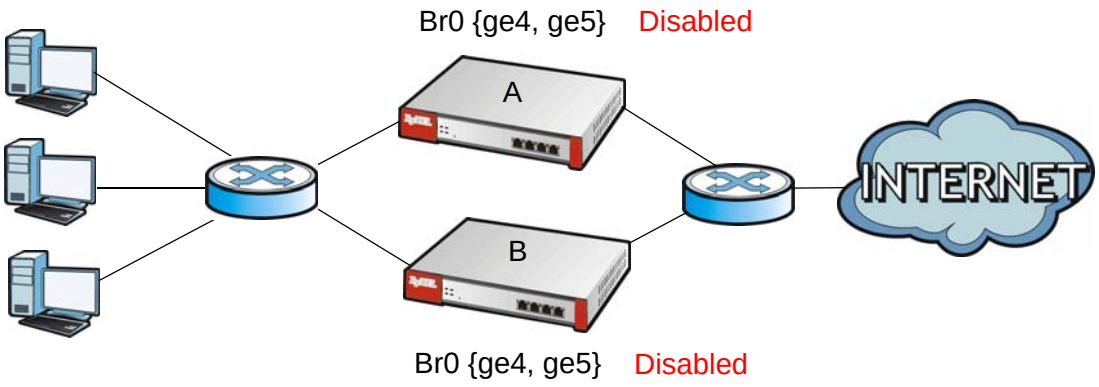
Second Option for Connecting the Bridge Interfaces on Two ZyWALLs

Another option is to disable the bridge interfaces, connect the bridge interfaces, activate device HA, and finally reactivate the bridge interfaces as shown in the following example.

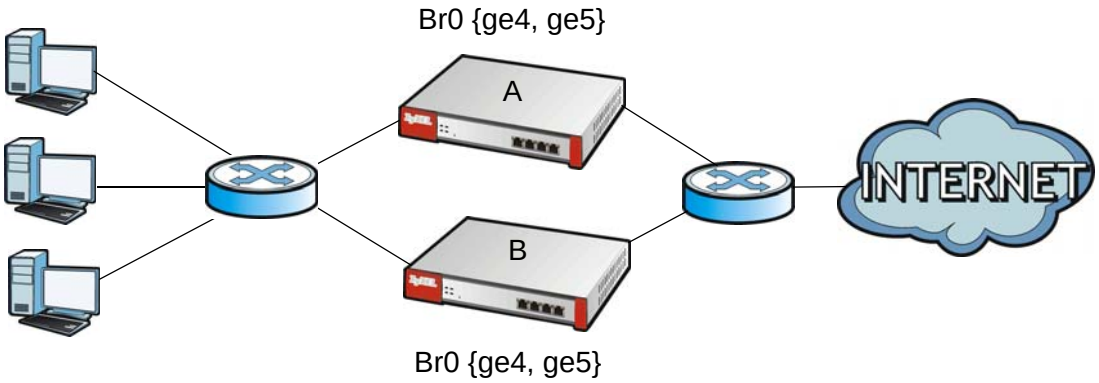
1 In this case the ZyWALLs are already connected, but the bridge faces have not been configured yet. Configure a disabled bridge interface on the master ZyWALL but disable it. Then set the bridge interface as a monitored interface, and activate device HA.



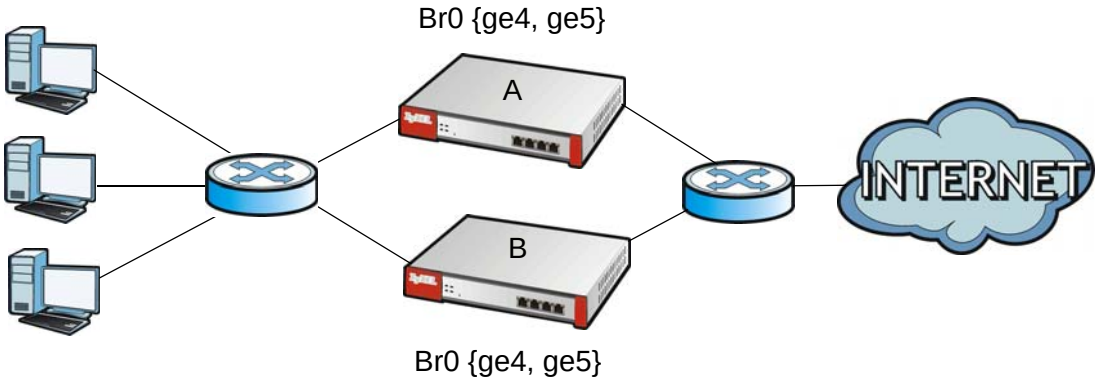
2 Configure a corresponding disabled bridge interface on the backup ZyWALL. Then set the bridge interface as a monitored interface, and activate device HA.



3 Enable the bridge interface on the master ZyWALL and then on the backup ZyWALL.



4 Connect the ZyWALLs.



Synchronization

During synchronization, the master ZyWALL sends the following information to the backup ZyWALL.

- Startup configuration file (**startup-config.conf**)
- Certificates (**My Certificates**, and **Trusted Certificates**)

Synchronization does not change the device HA settings in the backup ZyWALL.

Synchronization affects the entire device configuration. You can only configure one set of settings for synchronization, regardless of how many VRRP groups you might configure. The ZyWALL uses Secure FTP (on a port number you can change) to synchronize, but it is still recommended that the backup ZyWALL synchronize with a master ZyWALL on a secure network.

The backup ZyWALL gets the configuration from the master ZyWALL. The backup ZyWALL cannot become the master or be managed while it applies the new configuration. This usually takes two or three minutes or longer depending on the configuration complexity.

The following restrictions apply with active-passive mode.

- The master ZyWALL must have no inactive monitored interfaces.

- The backup ZyWALL cannot be the master. This refers to the actual role at the time of synchronization, not the role setting in the configuration screen.

27

User/Group

27.1 Overview

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL. You can also set up rules that control when users have to log in to the ZyWALL before the ZyWALL routes traffic for them.

27.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 27.2 on page 373) provides a summary of all user accounts.
- The **Group** screen (see Section 27.3 on page 376) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The **Setting** screen (see Section 27.4 on page 378) controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

27.1.2 What You Need To Know

User Account

A user account defines the privileges of a user logged into the ZyWALL. User accounts are used in firewall rules, in addition to controlling access to configuration and services in the ZyWALL.

User Types

These are the types of user accounts the ZyWALL uses.

Table 132 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 32 on page 409 for more information about authentication methods.)

Ext-User Accounts

Set up an **ext-user** account if the user is authenticated by an external server and you want to set up specific policies for this user in the ZyWALL. If you do not want to set up policies for this user, you do not have to set up an **ext-user** account.

All **ext-user** users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the ZyWALL tries to use the local database to authenticate an **ext-user**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in Chapter 31 on page 400 and Chapter 32 on page 409, respectively.)

Note: If the ZyWALL tries to authenticate an **ext-user** using the local database, the attempt always fails.

Once an **ext-user** user has been authenticated, the ZyWALL tries to get the user type (see Table 132 on page 371) from the external server. If the external server does not have the information, the ZyWALL sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the ZyWALL checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the ZyWALL.
3. Default user account for AD users (**ad-users**), LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the ZyWALL.

See Setting up User Attributes in an External Server on page 382 for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See Section 31.2.1 on page 403 for more on the group membership attribute.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the ZyWALL to use the network services it provides. The ZyWALL automatically routes packets for everyone. If you want to restrict network services that certain users can use via the ZyWALL, you can require them to log in to the ZyWALL first. The ZyWALL is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See Section 27.4.2 on page 381 for a user-aware login example.

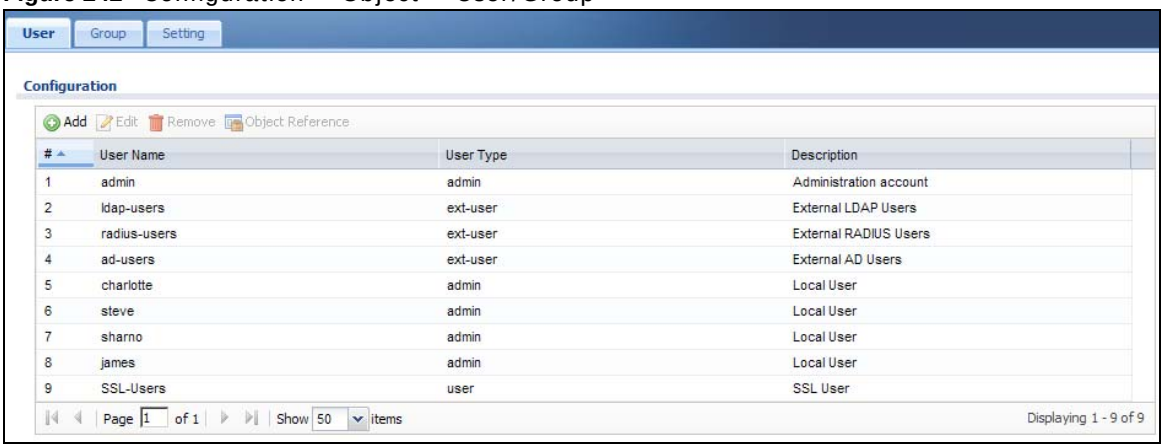
Finding Out More

- See Section 27.5 on page 382 for some information on users who use an external authentication server in order to log in.

27.2 User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group**.

Figure 242 Configuration > Object > User/Group


User
Group
Setting
Configuration
Add
Edit
Remove
Object Reference
| User Name | User Type | Description
1 | admin | admin | Administration account
2 | ldap-users | ext-user | External LDAP Users
3 | radius-users | ext-user | External RADIUS Users
4 | ad-users | ext-user | External AD Users
5 | charlotte | admin | Local User
6 | steve | admin | Local User
7 | sharno | admin | Local User
8 | james | admin | Local User
9 | SSL-Users | user | SSL User
Page 1 of 1
Show 50 items
Displaying 1 - 9 of 9

The following table describes the labels in this screen.

Table 133 Configuration > Object > User/Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.

Table 133 Configuration > Object > User/Group (continued)

LABEL	DESCRIPTION
User Type	This field displays the types of user accounts the ZyWALL uses: • **admin** - this user can look at and change the configuration of the ZyWALL • **limited-admin** - this user can look at the configuration of the ZyWALL but not to change it • **user** - this user has access to the ZyWALL's services and can also browse user-mode commands (CLI). • **guest** - this user has access to the ZyWALL's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 372 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 372 for more information about this type.
Description	This field displays the description for each user.

27.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

27.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

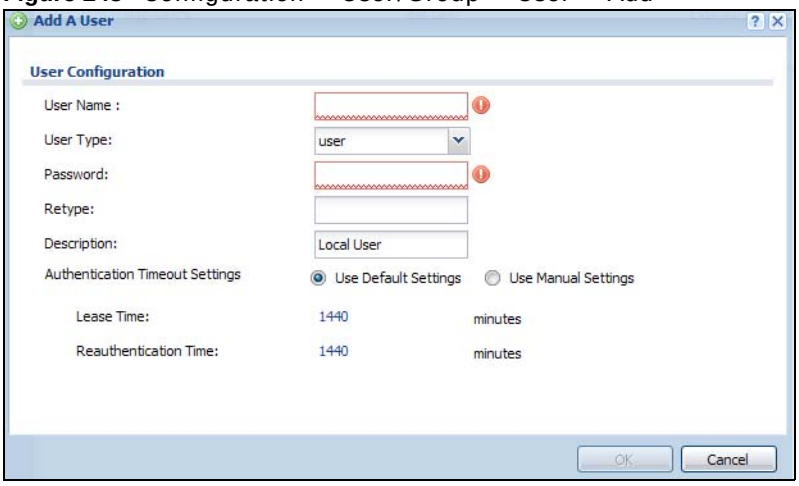
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• shutdown	• sshd
• sync	• uucp	• zyxel		

To access this screen, go to the **User** screen (see Section 27.2 on page 373), and click either the **Add** icon or an **Edit** icon.

Figure 243 Configuration > User/Group > User > Add



The following table describes the labels in this screen.

Table 134 Configuration > User/Group > User > Add

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 27.2.1.1 on page 374.
User Type	This field displays the types of user accounts the ZyWALL uses: • **admin** - this user can look at and change the configuration of the ZyWALL • **limited-admin** - this user can look at the configuration of the ZyWALL but not to change it • **user** - this user has access to the ZyWALL's services and can also browse user-mode commands (CLI). • **guest** - this user has access to the ZyWALL's services but cannot look at the configuration. • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 372 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 372 for more information about this type.
Password	This field is not available if you select the **ext-user** or **ext-group-user** type. Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.
Retype	This field is not available if you select the **ext-user** or **ext-group-user** type.
Group Identifier	This field is available for a **ext-group-user** type user account. Specify the value of the AD or LDAP server's **Group Membership Attribute** that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a **ext-group-user** type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	If you want the system to use default settings, select **Use Default Settings**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.

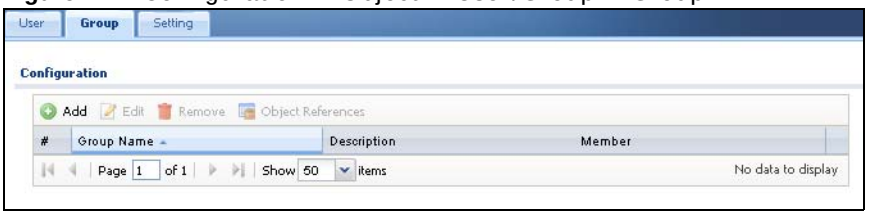
Table 134 Configuration > User/Group > User > Add (continued)

LABEL	DESCRIPTION
Lease Time	If you select **Use Default Settings** in the **Authentication Timeout Settings** field, the default lease time is shown. If you select **Use Manual Settings**, you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 27.4 on page 378), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select **Use Default Settings** in the **Authentication Timeout Settings** field, the default lease time is shown. If you select **Use Manual Settings**, you need to type the number of minutes this user can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the **User Name** field and click **Test**.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.3 User Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Group**.

Figure 244 Configuration > Object > User/Group > Group



The following table describes the labels in this screen. See Section 27.3.1 on page 377 for more information as well.

Table 135 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.

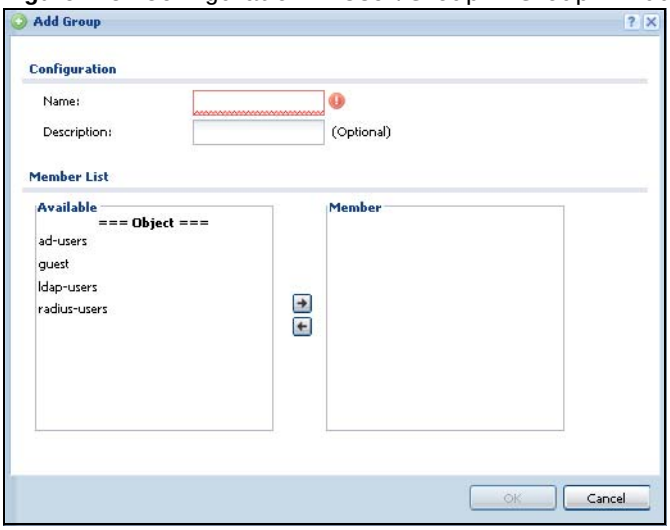
Table 135 Configuration > Object > User/Group > Group (continued)

LABEL	DESCRIPTION
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.

27.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see Section 27.3 on page 376), and click either the **Add** icon or an **Edit** icon.

Figure 245 Configuration > User/Group > Group > Add



The following table describes the labels in this screen.

Table 136 Configuration > User/Group > Group > Add

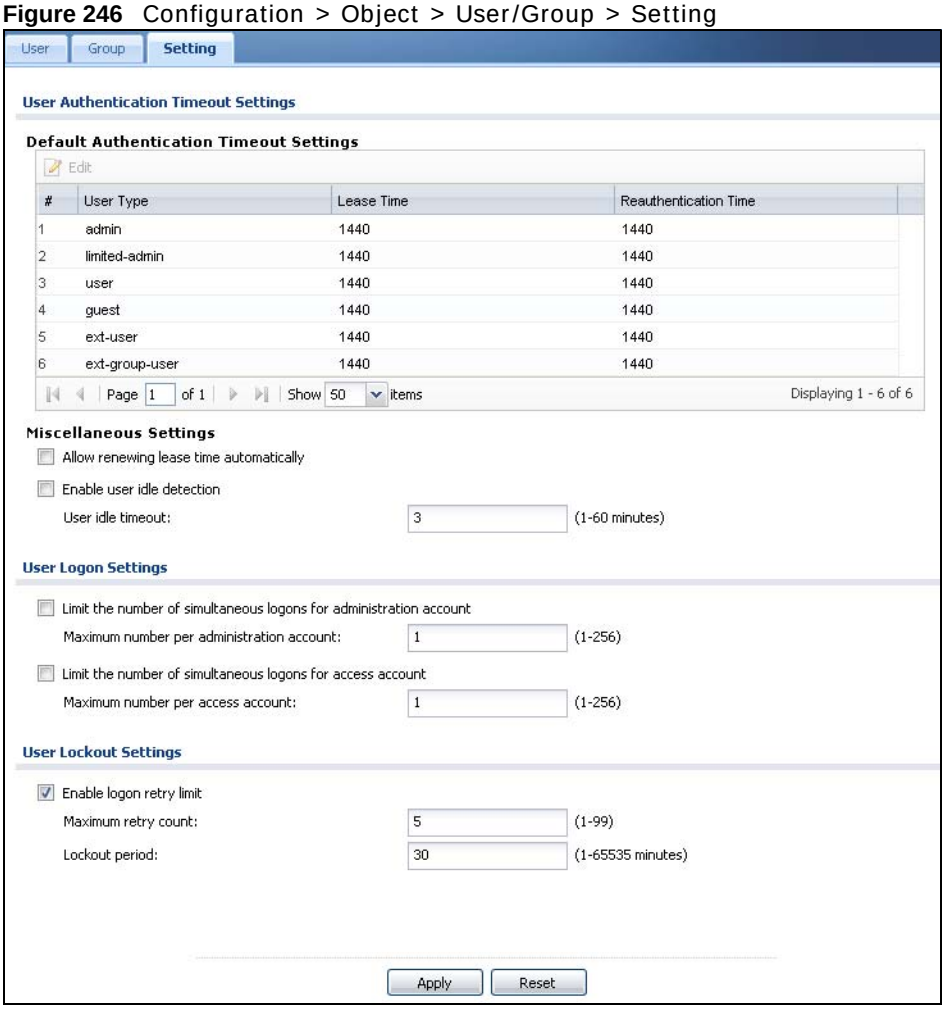
LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The **Member** list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the **Available** list that you want to be members of this group and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.4 The User/Group Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Setting**.

Figure 246 Configuration > Object > User/Group > Setting


User
Group
Setting
User Authentication Timeout Settings
Default Authentication Timeout Settings
Edit
User Type Lease Time Reauthentication Time
1 admin 1440 1440
2 limited-admin 1440 1440
3 user 1440 1440
4 guest 1440 1440
5 ext-user 1440 1440
6 ext-group-user 1440 1440
Page 1 of 1 Show 50 items
Displaying 1 - 6 of 6
Miscellaneous Settings
Allow renewing lease time automatically
Enable user idle detection
User idle timeout: 3 (1-60 minutes)
User Logon Settings
Limit the number of simultaneous logons for administration account
Maximum number per administration account: 1 (1-256)
Limit the number of simultaneous logons for access account
Maximum number per access account: 1 (1-256)
User Lockout Settings
Enable logon retry limit
Maximum retry count: 5 (1-99)
Lockout period: 30 (1-65535 minutes)
Apply
Reset

The following table describes the labels in this screen.

Table 137 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.

Table 137 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the ZyWALL supports. • **admin** - this user can look at and change the configuration of the ZyWALL • **limited-admin** - this user can look at the configuration of the ZyWALL but not to change it • **user** - this user has access to the ZyWALL's services but cannot look at the configuration • **guest** - this user has access to the ZyWALL's services but cannot look at the configuration • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 372 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 372 for more information about this type.
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 27.4 on page 378), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the ZyWALL in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Miscellaneous Settings	
Allow renewing lease time automatically	Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the **Updating lease time automatically** check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the ZyWALL to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ZyWALL automatically logs out the access user once the **User idle timeout** has been reached.
User idle timeout	This is applicable for access users. This field is effective when **Enable user idle detection** is checked. Type the number of minutes each access user can be logged in and idle before the ZyWALL automatically logs out the access user.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user.
Limit the number of simultaneous logons for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.

Table 137 Configuration > Object > User/Group > Setting (continued)

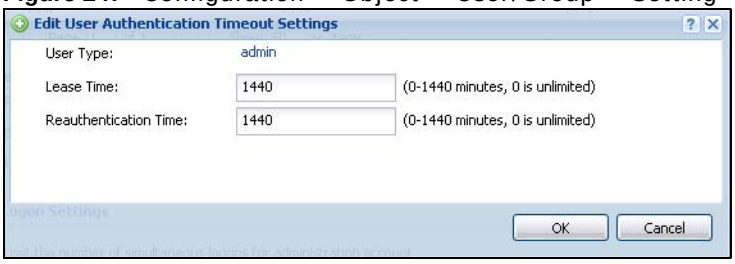
LABEL	DESCRIPTION
Maximum number per access account	This field is effective when **Limit ... for access account** is checked. Type the maximum number of simultaneous logins by each access user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

27.4.1 Default User Authentication Timeout Settings Edit Screens

The **Default Authentication Timeout Settings Edit** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User/Group > Setting** screen (see Section 27.4 on page 378), and click one of the **Default Authentication Timeout Settings** section's **Edit** icons.

Figure 247 Configuration > Object > User/Group > Setting > Edit



The following table describes the labels in this screen.

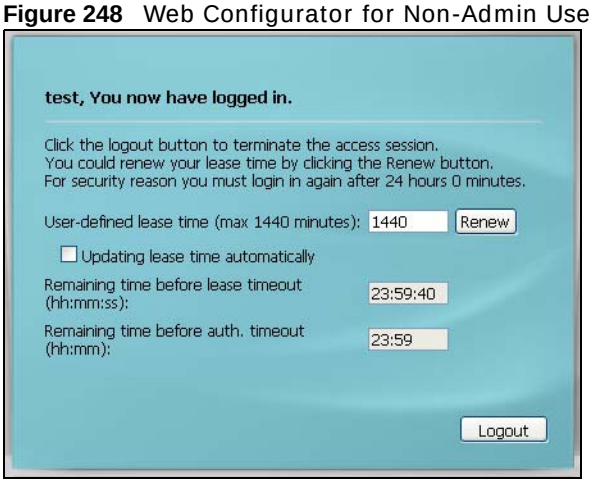
Table 138 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the ZyWALL • **limited-admin** - this user can look at the configuration of the ZyWALL but not to change it. • **user** - this user has access to the ZyWALL's services but cannot look at the configuration. • **guest** - this user has access to the ZyWALL's services but cannot look at the configuration. • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 372 for more information about this type. • **ext-group-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 372 for more information about this type.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 27.4 on page 378), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

27.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the ZyWALL. Instead, after access users log into the ZyWALL, the following screen appears.

Figure 248 Web Configurator for Non-Admin Users


test, You now have logged in.
Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 24 hours 0 minutes.
User-defined lease time (max 1440 minutes):
1440
Renew
Updating lease time automatically
Remaining time before lease timeout (hh:mm:ss):
23:59:40
Remaining time before auth. timeout (hh:mm):
23:59
Logout

The following table describes the labels in this screen.

Table 139 Web Configurator for Non-Admin Users

LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the ZyWALL automatically logs them out. The ZyWALL sets this amount of time according to the • **User-defined lease time** field in this screen • **Lease time** field in the **User Add/Edit** screen (see Section 27.2.1 on page 374) • **Lease time** field in the **Setting** screen (see Section 27.4 on page 378)
Updating lease time automatically	This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 27.4 on page 378.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the **Renew** button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the ZyWALL automatically logs the access user out, regardless of the lease time.

27.5 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 140 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	**User Type**. Possible Values: admin, limited-admin, user, guest.
leaseTime	**Lease Time**. Possible Values: 1-1440 (minutes).
reauthTime	**Reauthentication Time**. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 249 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 250 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts. See Chapter 39 on page 499 for more information about shell scripts.

28

Addresses

28.1 Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

28.1.1 What You Can Do in this Chapter

- The **Address** screen (Section 28.2 on page 384) provides a summary of all addresses in the ZyWALL. Use the **Address Add / Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen (Section 28.3 on page 388) and the **Address Group Add / Edit** screen, to maintain address groups in the ZyWALL.

28.1.2 What You Need To Know

Address objects and address groups are used in dynamic routes, firewall rules, and VPN connection policies. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

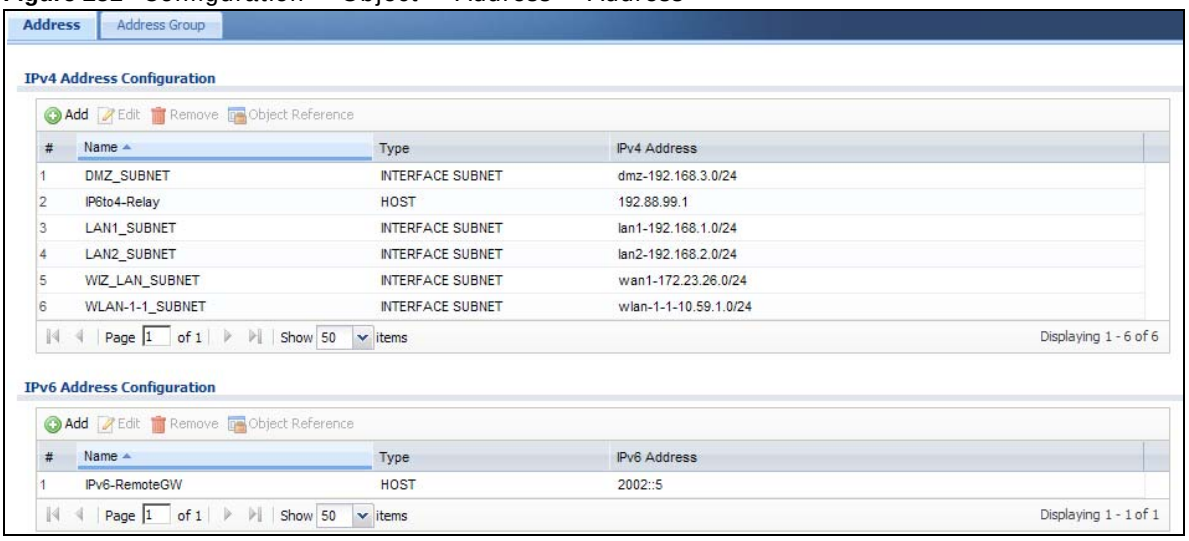
28.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network** IP address and **Netmask** subnet mask.

The **Address** screen provides a summary of all addresses in the ZyWALL. To access this screen, click **Configuration > Object** > **Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 251 Configuration > Object > Address > Address



The following table describes the labels in this screen. See Section 28.2.1 on page 386 for more information as well.

Table 141 Configuration > Object > Address > Address

LABEL	DESCRIPTION
IPv4 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the ZyWALL's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the ZyWALL's interfaces, the name of the interface displays first followed by the object's current address settings.
IPv6 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object References** to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.

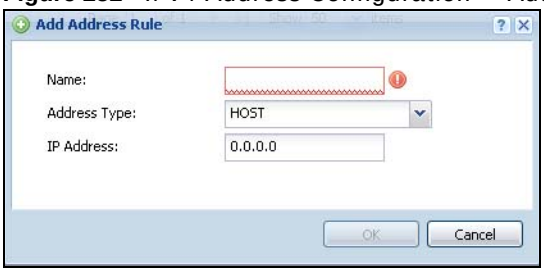
Table 141 Configuration > Object > Address > Address (continued)

LABEL	DESCRIPTION
Type	This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the ZyWALL's interfaces.
IPv6 Address	This field displays the IPv6 addresses represented by each address object. If the object's settings are based on one of the ZyWALL's interfaces, the name of the interface displays first followed by the object's current address settings.

28.2.1 IPv4 Address Add/Edit Screen

The **Configuration > IPv4 Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 28.2 on page 384), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Configuration** section.

Figure 252 IPv4 Address Configuration > Add/Edit



The following table describes the labels in this screen.

Table 142 IPv4 Address Configuration > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: **HOST**, **RANGE**, **SUBNET**, **INTERFACE IP**, **INTERFACE SUBNET**, and **INTERFACE GATEWAY**. Note: The ZyWALL automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents.

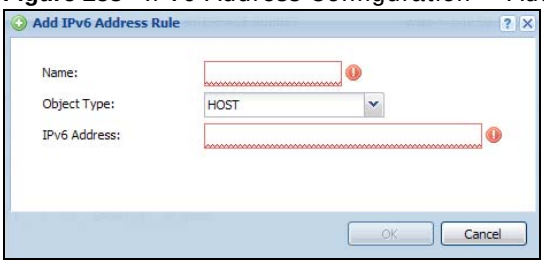
Table 142 IPv4 Address Configuration > Add/Edit (continued)

LABEL	DESCRIPTION
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

28.2.2 IPv6 Address Add/Edit Screen

The **Configuration > IPv6 Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 28.2 on page 384), and click either the **Add** icon or an **Edit** icon in the **IPv6 Address Configuration** section.

Figure 253 IPv6 Address Configuration > Add/Edit



The following table describes the labels in this screen.

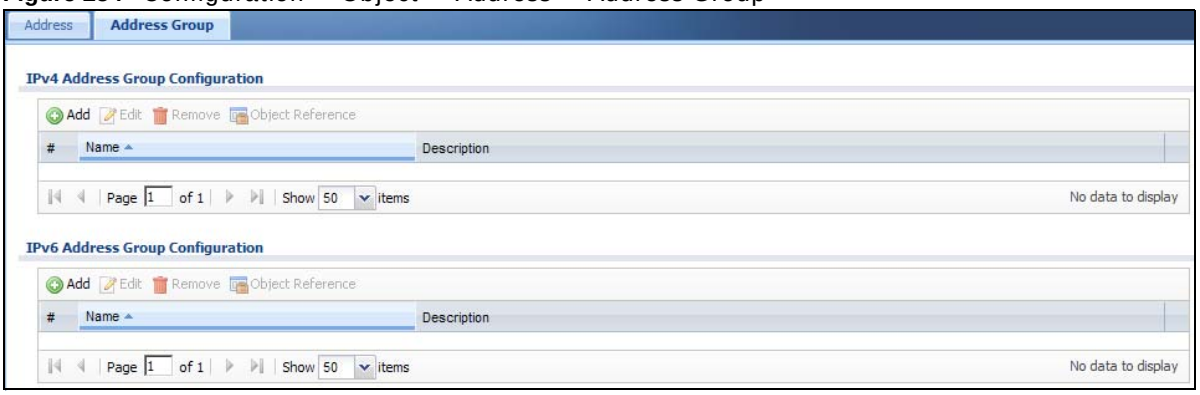
Table 143 IPv6 Address Configuration > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Object Type	Select the type of address you want to create. Choices are: **HOST**, **RANGE**, **SUBNET**, **INTERFACE IP**, **INTERFACE SUBNET**, and **INTERFACE GATEWAY**. Note: The ZyWALL automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN subnet address object.
IPv6 Address	This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents.
IPv6 Starting Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
IPv6 Ending Address	This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
IPv6 Address Prefix	This field is only available if the **Address Type** is **SUBNET**. This field cannot be blank. Enter the IPv6 address prefix that the ZyWALL uses for the LAN IPv6 address.
Interface	If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents.
IPv6 Address Type	Select whether the IPv6 address is a link-local IP address (**LINK LOCAL**), static IP address (**STATIC**), an IPv6 StateLess Address Auto Configuration IP address (**SLAAC**), or is obtained from a DHCPv6 server (**DHCPv6**).
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

28.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Configuration > Object** > **Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 254 Configuration > Object > Address > Address Group



The following table describes the labels in this screen. See Section 28.3.1 on page 389 for more information as well.

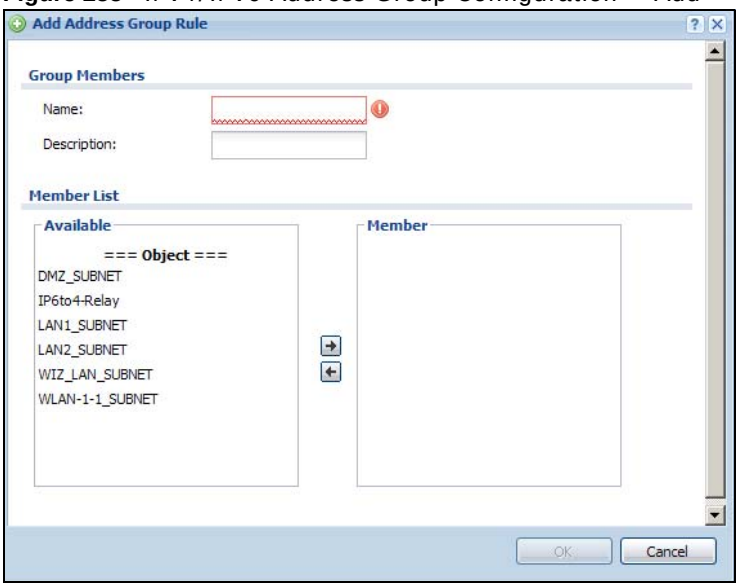
Table 144 Configuration > Object > Address > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
IPv6 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.

28.3.1 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see Section 28.3 on page 388), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Group Configuration** or **IPv6 Address Group Configuration** section.

Figure 255 IPv4/IPv6 Address Group Configuration > Add



The following table describes the labels in this screen.

Table 145 IPv4/IPv6 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The **Member** list displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

29

Services

29.1 Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

29.1.1 What You Can Do in this Chapter

- Use the **Service** screens (Section 29.2 on page 391) to view and configure the ZyWALL's list of services and their definitions.
- Use the **Service Group** screens (Section 29.2 on page 391) to view and configure the ZyWALL's list of service groups.

29.1.2 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, firewall rules.

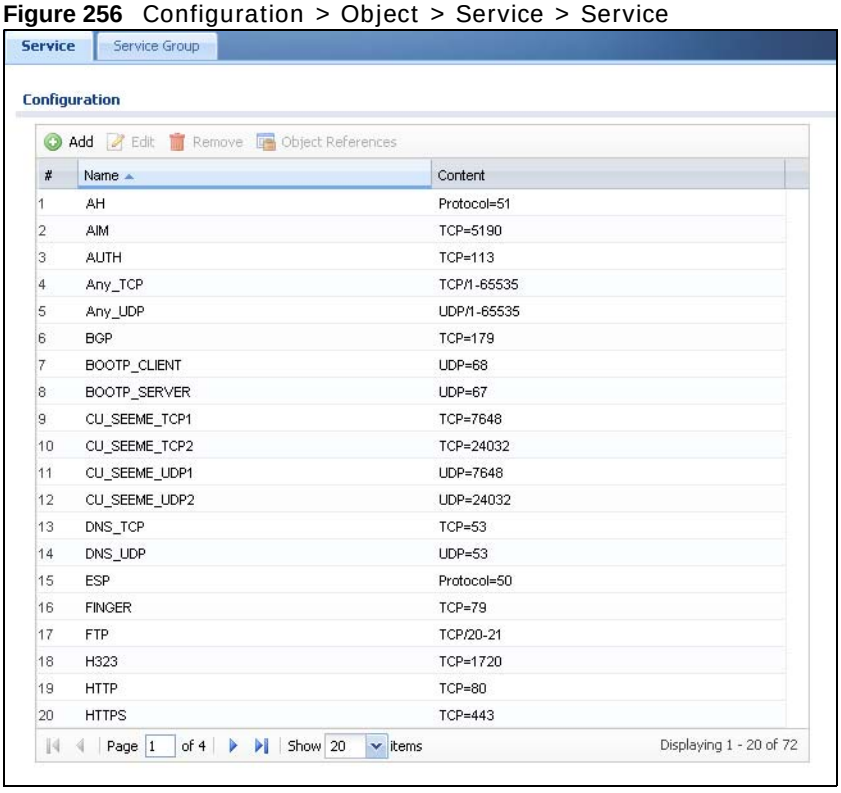
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

29.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 256 Configuration > Object > Service > Service



The following table describes the labels in this screen.

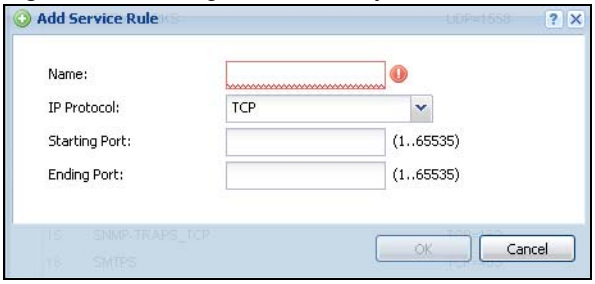
Table 146 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.

29.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see Section 29.2 on page 391), and click either the **Add** icon or an **Edit** icon.

Figure 257 Configuration > Object > Service > Service > Edit



The following table describes the labels in this screen.

Table 147 Configuration > Object > Service > Service > Edit

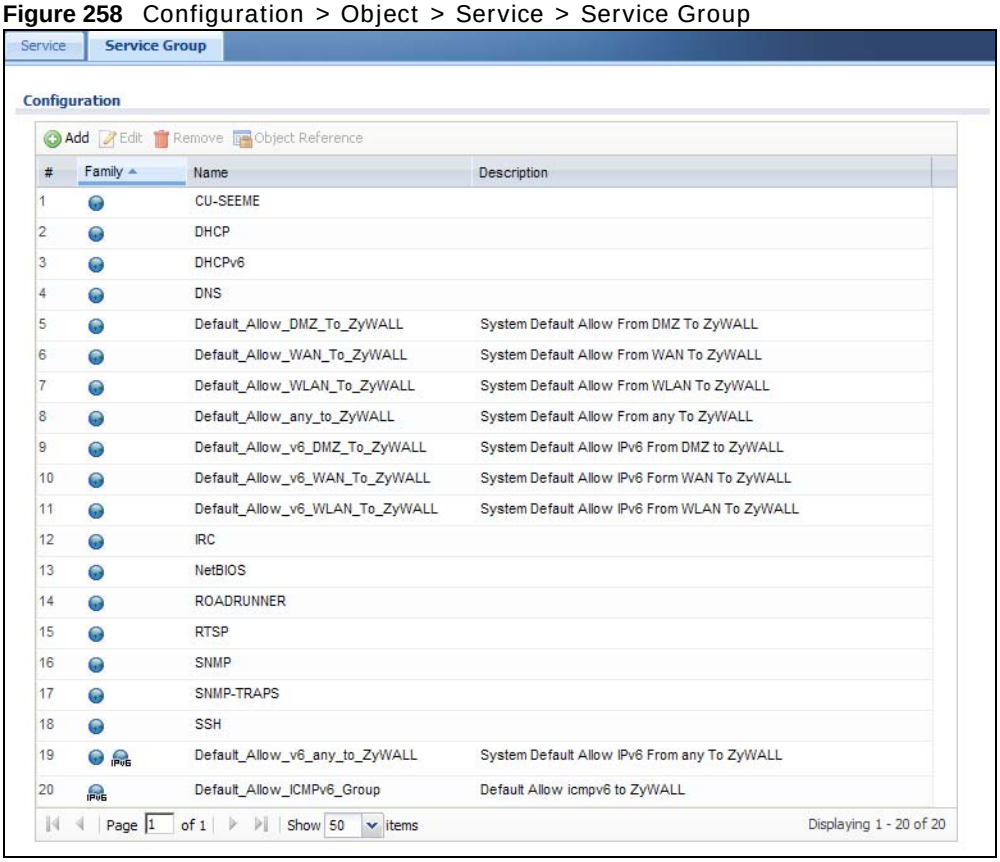
LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **User Defined**.
Starting Port Ending Port	This field appears if the **IP Protocol** is **TCP** or **UDP**. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the **IP Protocol** is **ICMP** or **ICMPv6**. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the **IP Protocol** is **User Defined**. Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

29.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the Web Configurator, and click **Configuration > Object** > **Service** > **Service Group**.

Figure 258 Configuration > Object > Service > Service Group


Service
Service Group
Configuration
Add
Edit
Remove
Object Reference
Family Name Description
1 CU-SEEME
2 DHCP
3 DHCPv6
4 DNS
5 Default_Allow_DMZ_To_ZyWALL System Default Allow From DMZ To ZyWALL
6 Default_Allow_WAN_To_ZyWALL System Default Allow From WAN To ZyWALL
7 Default_Allow_WLAN_To_ZyWALL System Default Allow From WLAN To ZyWALL
8 Default_Allow_any_to_ZyWALL System Default Allow From any To ZyWALL
9 Default_Allow_v6_DMZ_To_ZyWALL System Default Allow IPv6 From DMZ to ZyWALL
10 Default_Allow_v6_WAN_To_ZyWALL System Default Allow IPv6 Form WAN To ZyWALL
11 Default_Allow_v6_WLAN_To_ZyWALL System Default Allow IPv6 From WLAN To ZyWALL
12 IRC
13 NetBIOS
14 ROADRUNNER
15 RTSP
16 SNMP
17 SNMP-TRAPS
18 SSH
19 Default_Allow_v6_any_to_ZyWALL System Default Allow IPv6 From any To ZyWALL
20 Default_Allow_ICMPv6_Group Default Allow icmpv6 to ZyWALL
Page 1 of 1
Show 50 items
Displaying 1 - 20 of 20

The following table describes the labels in this screen. See Section 29.3.1 on page 394 for more information as well.

Table 148 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific service group.

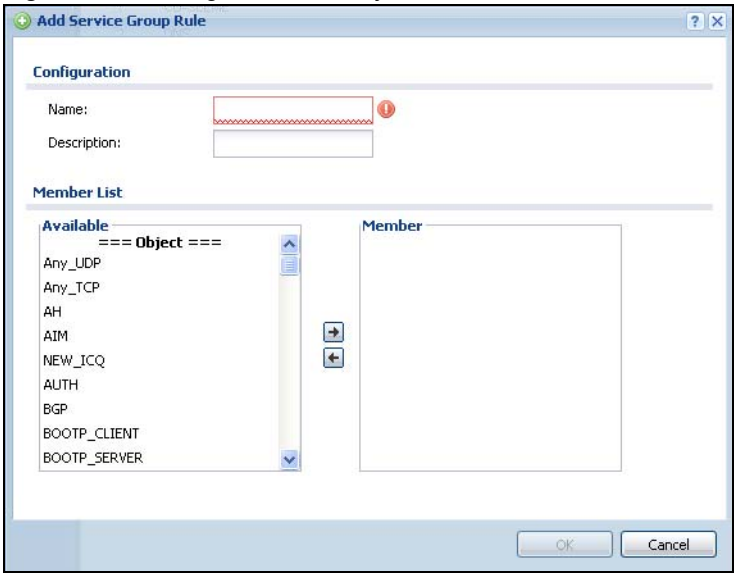
Table 148 Configuration > Object > Service > Service Group (continued)

LABEL	DESCRIPTION
Family	This field displays the Server Group supported type, which is according to your configurations in the **Service Group Add / Edit** screen. There are 3 types of families: • : Supports IPv4 only • : Supports IPv6 only • : Supports both IPv4 and IPv6
Name	This field displays the name of each service group. By default, the ZyWALL uses services starting with “Default_Allow_” in the firewall rules to allow certain services to connect to the ZyWALL.
Description	This field displays the description of each service group, if any.

29.3.1 The Service Group Add/Edit Screen

The **Service Group Add / Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see Section 29.3 on page 393), and click either the **Add** icon or an **Edit** icon.

Figure 259 Configuration > Object > Service > Service Group > Edit



The following table describes the labels in this screen.

Table 149 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.

Table 149 Configuration > Object > Service > Service Group > Edit (continued)

LABEL	DESCRIPTION
Member List	The **Member** list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the **Available** list that you want to be members and move them to the **Member** list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the **Available** list.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

30

Schedules

30.1 Overview

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules. The ZyWALL supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ZyWALL.

Note: Schedules are based on the ZyWALL's current date and time.

30.1.1 What You Can Do in this Chapter

- Use the **Schedule** summary screen (Section 30.2 on page 397) to see a list of all schedules in the ZyWALL.
- Use the **One-Time Schedule Add / Edit** screen (Section 30.2.1 on page 398) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add / Edit** screen (Section 30.2.2 on page 399) to create or edit a recurring schedule.

30.1.2 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

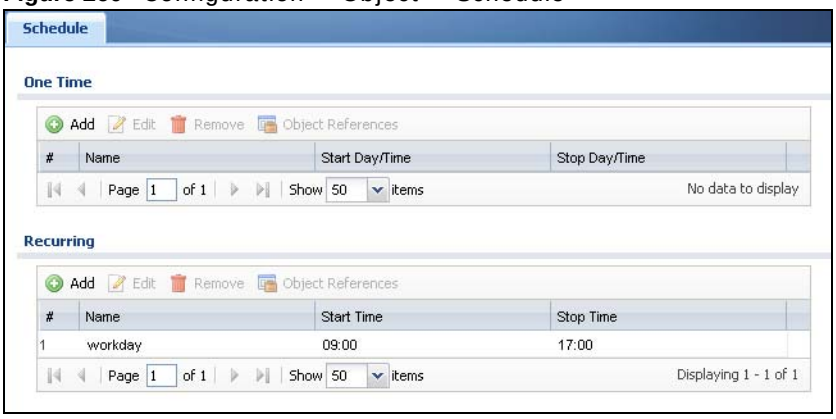
Finding Out More

- See Section 37.4 on page 445 for information about the ZyWALL's current date and time.

30.2 The Schedule Summary Screen

The **Schedule** summary screen provides a summary of all schedules in the ZyWALL. To access this screen, click **Configuration > Object** > **Schedule**.

Figure 260 Configuration > Object > Schedule



The following table describes the labels in this screen. See Section 30.2.1 on page 398 and Section 30.2.2 on page 399 for more information as well.

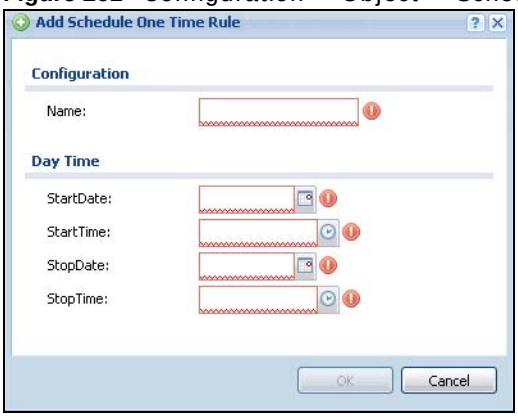
Table 150 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.

30.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 30.2 on page 397), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 261 Configuration > Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

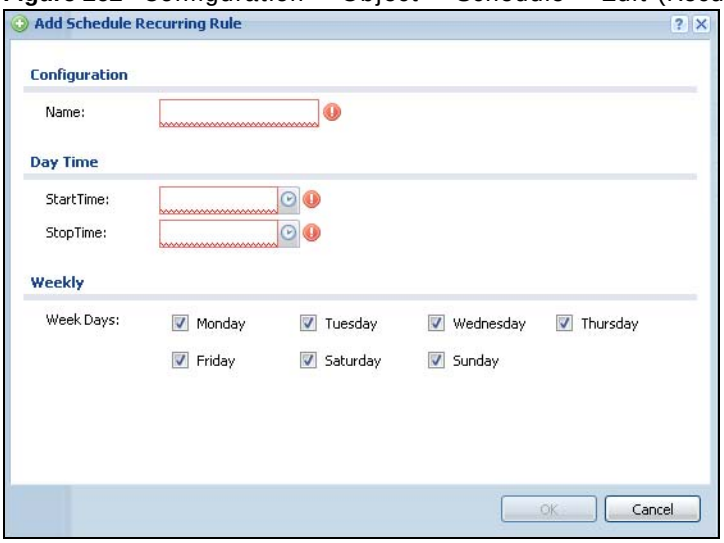
Table 151 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartDate	Specify the year, month, and day when the schedule begins. • **Year** - 1900 - 2999 • **Month** - 1 - 12 • **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. • **Hour** - 0 - 23 • **Minute** - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. • **Year** - 1900 - 2999 • **Month** - 1 - 12 • **Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. • **Hour** - 0 - 23 • **Minute** - 0 - 59
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

30.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 30.2 on page 397), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 262 Configuration > Object > Schedule > Edit (Recurring)



The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

Table 152 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. • **Hour** - 0 - 23 • **Minute** - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. • **Hour** - 0 - 23 • **Minute** - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

31

AAA Server

31.1 Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You use AAA server objects in configuring ext-group-user user objects and authentication method objects (see Chapter 32 on page 409).

31.1.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the ZyWALL) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 263 Example: Directory Service Client and Server



The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The ZyWALL tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the ZyWALL checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

31.1.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 264 RADIUS Server Network Example



31.1.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a ZyWALL OTP package in order to use this feature. The package contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1. Install the ASAS server software on a computer.
2. Create user accounts on the ZyWALL and in the ASAS server.
3. Import each token's database file (located on the included CD) into the server.
4. Assign users to OTP tokens (on the ASAS server).
5. Configure the ASAS as a RADIUS server in the ZyWALL's **Configuration > Object > AAA Server** screens.
6. Give the OTP tokens to (local or remote) users.

31.1.4 What You Can Do in this Chapter

- Use the **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) screens (Section 31.2 on page 403) to configure Active Directory or LDAP server objects.
- Use the **Configuration > Object > AAA Server > RADIUS** screen (Section 31.3 on page 406) to configure the default external RADIUS server to use for user authentication.

31.1.5 What You Need To Know

AAA Servers Supported by the ZyWALL

The following lists the types of authentication server the ZyWALL supports.

- Local user database

  The ZyWALL uses the built-in local user database to authenticate administrative users logging into the ZyWALL's Web Configurator or network access users logging into the network through the ZyWALL. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

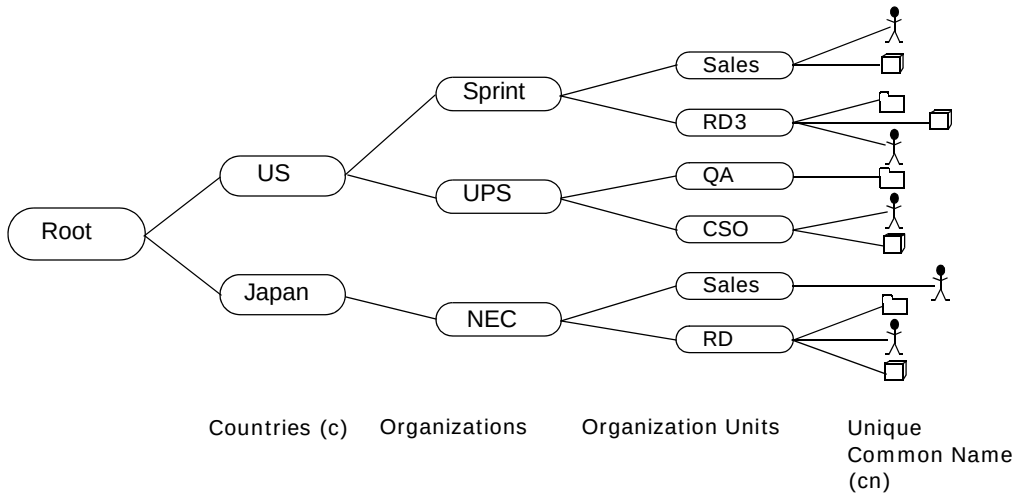
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 265 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("`cn=domain1.com, ou=Sales, o=MyCompany`" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany, c=UK` where `o` means organization and `c` means country.

Bind DN

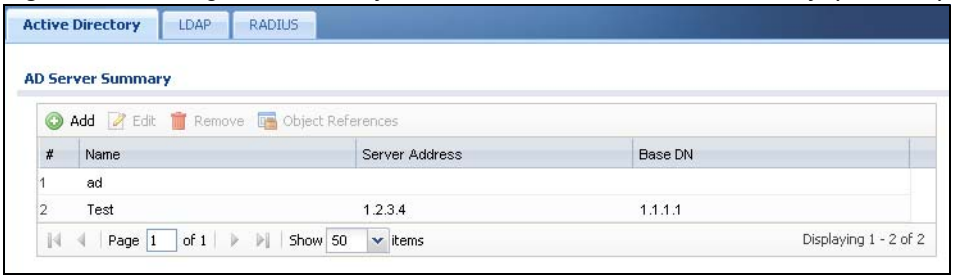
A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=zywallAdmin` allows the ZyWALL to log into the LDAP/AD server using the user name of `zywallAdmin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the ZyWALL will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

31.2 Active Directory or LDAP Server Summary

Use the **Active Directory** or **LDAP** screen to manage the list of AD or LDAP servers the ZyWALL can use in authenticating users.

Click **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen.

Figure 266 Configuration > Object > AAA Server > Active Directory (or LDAP)



The following table describes the labels in this screen.

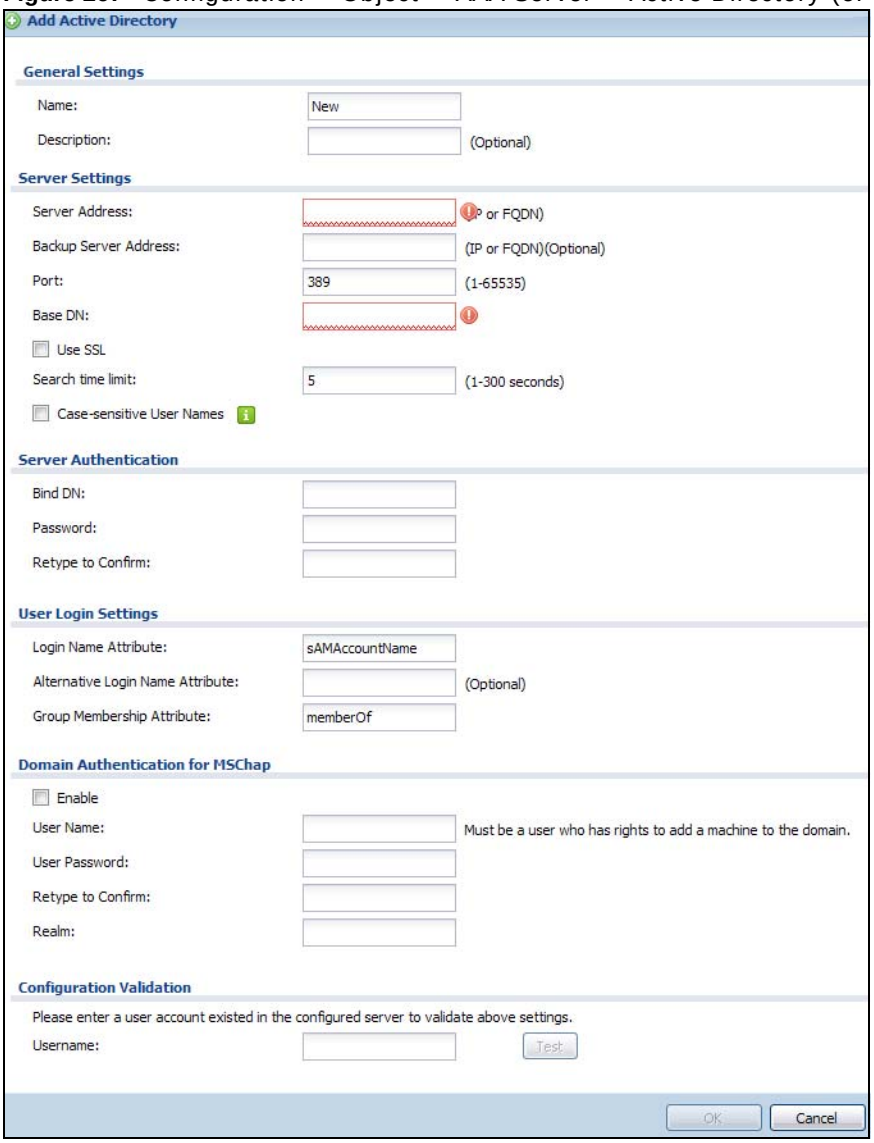
Table 153 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the index number.
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, `o=ZyXEL, c=US`.

31.2.1 Adding an Active Directory or LDAP Server

Click **Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 267 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add



The following table describes the labels in this screen.

Table 154 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.
Port	Specify the port number on the AD or LDAP server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.

Table 154 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

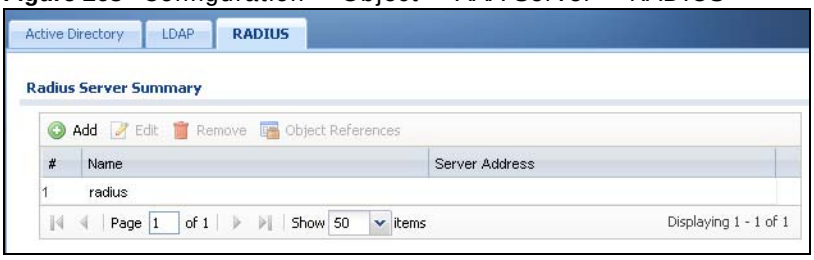
LABEL	DESCRIPTION
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, o=ZyXEL, c=US. This is only for **LDAP**.
Use SSL	Select **Use SSL** to establish a secure connection to the AD or LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the usernames.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, cn=zywallAdmin specifies zywallAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the ZyWALL to bind (or log in) to the AD or LDAP server.
Retype to Confirm	Retype your new password for confirmation.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example “name” or “e-mail address”.
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example “name” or “e-mail address”.
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the ZyWALL is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create a **ext-group-user** user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”.
Domain Authentication for MSChap	Select the **Enable** checkbox to enable domain authentication for MSChap. This is only for **Active Directory**.
User Name	Enter the user name for the user who has rights to add a machine to the domain. This is only for **Active Directory**.
User Password	Enter the password for the associated user name. This is only for **Active Directory**.
Retype to Confirm	Retype your new password for confirmation. This is only for **Active Directory**.
Realm	Enter the realm FQDN. This is only for **Active Directory**.
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account’s user name in the **Username** field and click **Test**.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

31.3 RADIUS Server Summary

Use the **RADIUS** screen to manage the list of RADIUS servers the ZyWALL can use in authenticating users.

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen.

Figure 268 Configuration > Object > AAA Server > RADIUS



The following table describes the labels in this screen.

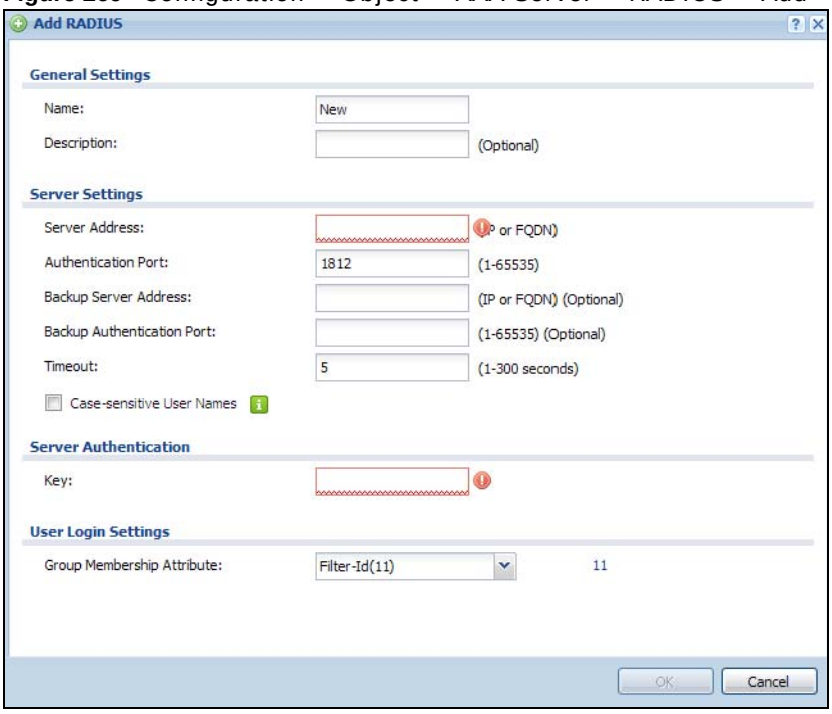
Table 155 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the AD or LDAP server.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

31.3.1 Adding a RADIUS Server

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 269 Configuration > Object > AAA Server > RADIUS > Add



The following table describes the labels in this screen.

Table 156 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and the ZyWALL.

Table 156 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the ZyWALL is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add **ext-group-user** user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a **ext-group-user** user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

32

Authentication Method

32.1 Overview

Authentication method objects set how the ZyWALL authenticates wireless, HTTP/HTTPS clients, and peer IPSec routers (extended authentication) clients. Configure authentication method objects to have the ZyWALL use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the ZyWALL are authenticated locally.

32.1.1 What You Can Do in this Chapter

- Use the **Configuration > Object > Auth. Method** screens (Section 32.2 on page 410) to create and manage authentication method objects.

Finding Out More

32.1.2 Before You Begin

Configure AAA server objects (see Chapter 31 on page 400) before you configure authentication method objects.

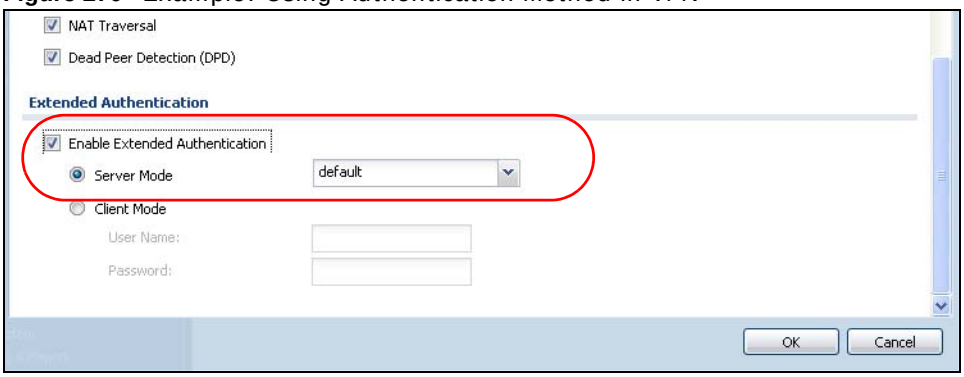
32.1.3 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

1. Access the **Configuration > VPN > IPSec VPN > VPN Gateway** > **Edit** screen.
2. Click **Show Advance Setting** and select **Enable Extended Authentication**.
3. Select **Server Mode** and select an authentication method object from the drop-down list box.
4. Click **OK** to save the settings.

Figure 270 Example: Using Authentication Method in VPN

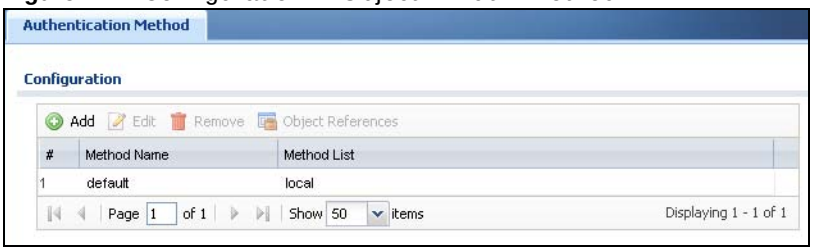


32.2 Authentication Method Objects

Click **Configuration > Object > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication method objects.

Figure 271 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 157 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.

32.2.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

1 Click **Configuration > Object > Auth. Method**.

2 Click **Add**.

3 Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.

4 Click **Add** to insert an authentication method in the table.

5 Select a server object from the **Method List** drop-down list box.

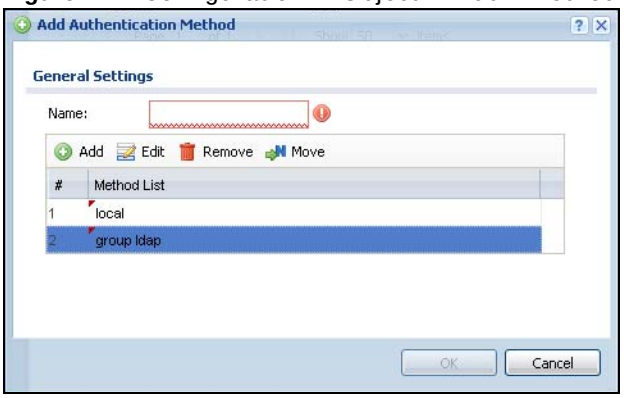
6 You can add up to four server objects to the table. The ordering of the **Method List** column is important. The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server.

Note: You can NOT select two server objects of the same type.

7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 272 Configuration > Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 158 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.

Table 158 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Move	To change a method's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as ZyWALL authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the **AAA Server** screen (see Chapter 31 on page 400 for more information). The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard the changes.

33

Certificates

33.1 Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

33.1.1 What You Can Do in this Chapter

- Use the **My Certificates** screens (see Section 33.2 on page 416 to Section 33.2.3 on page 422) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the **Trusted Certificates** screens (see Section 33.3 on page 423 to Section 33.3.2 on page 427) to save CA certificates and trusted remote host certificates to the ZyWALL. The ZyWALL trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

33.1.2 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the ZyWALL act as a certification authority and sign its own certificates.

Factory Default Certificate

The ZyWALL generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

Finding Out More

- See Section 33.4 on page 428 for certificate background information.

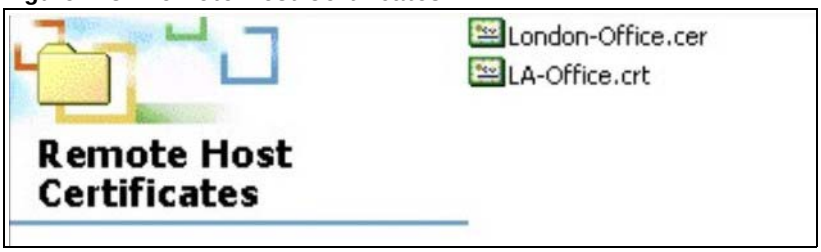
33.1.3 Verifying a Certificate

Before you import a trusted certificate into the ZyWALL, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

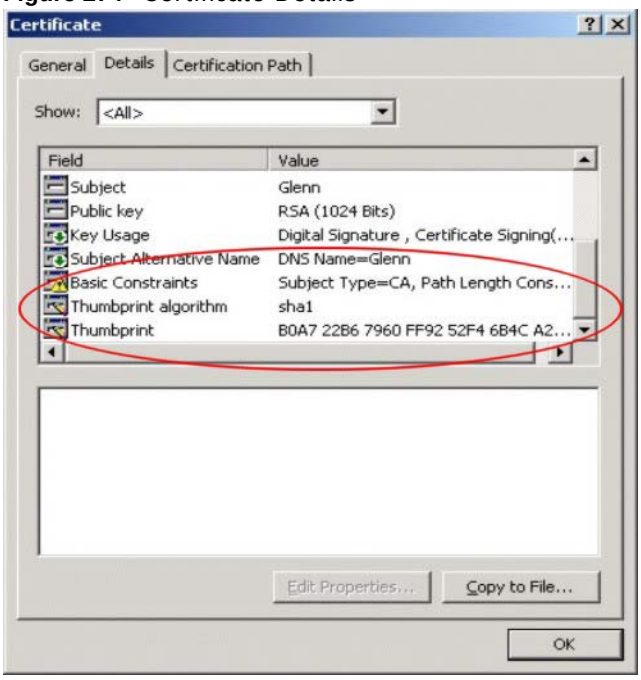
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 273 Remote Host Certificates



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 274 Certificate Details

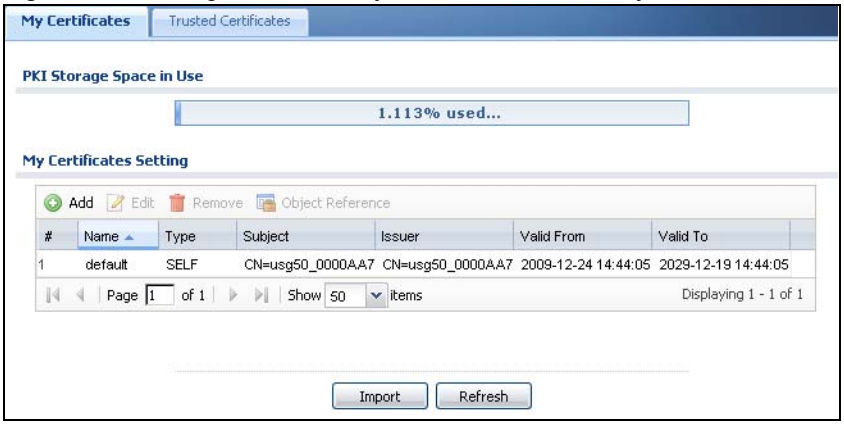


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

33.2 The My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests.

Figure 275 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

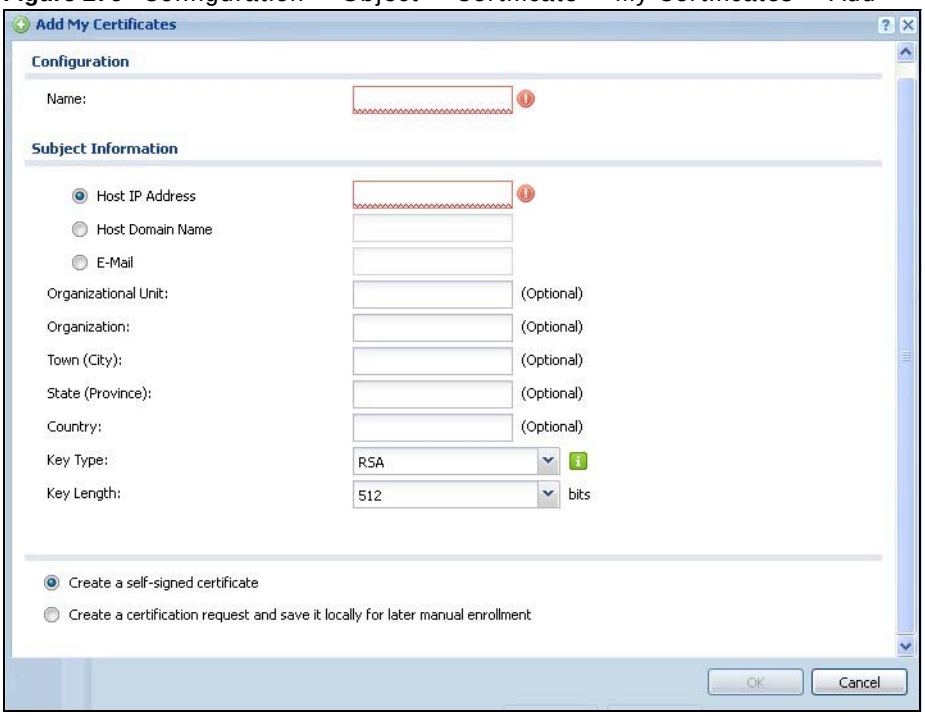
Table 159 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the ZyWALL generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the ZyWALL's features are configured to use. Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the ZyWALL.
Refresh	Click **Refresh** to display the current validity status of the certificates.

33.2.1 The My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the ZyWALL create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 276 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 160 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 160 Configuration > Object > Certificate > My Certificates > Add (continued)

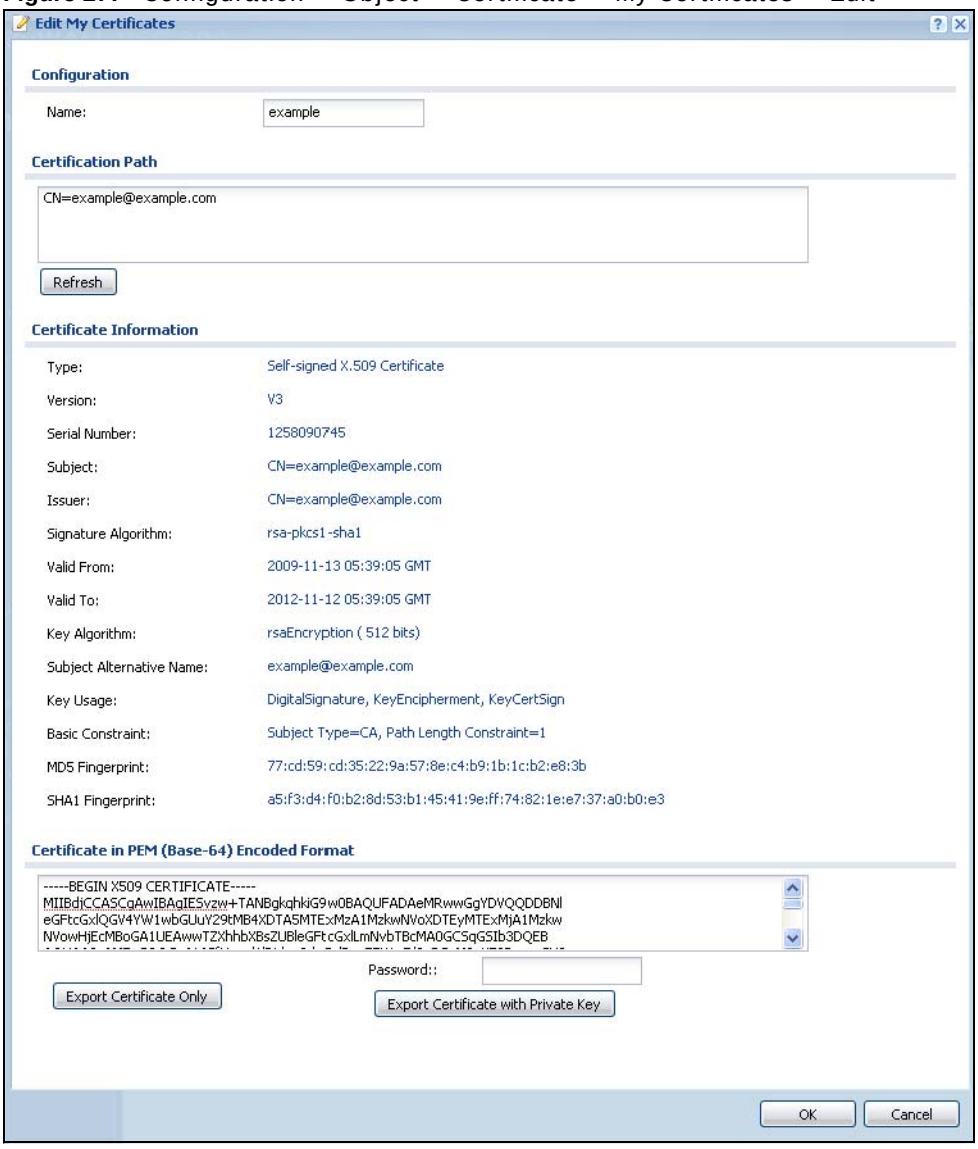
LABEL	DESCRIPTION
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm. Select **DSA** to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 33.2.2 on page 419) and then send it to the certification authority.
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

33.2.2 The My Certificates Edit Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 277 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 161 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{},.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.

Table 161 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).

Table 161 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

33.2.3 The My Certificates Import Screen

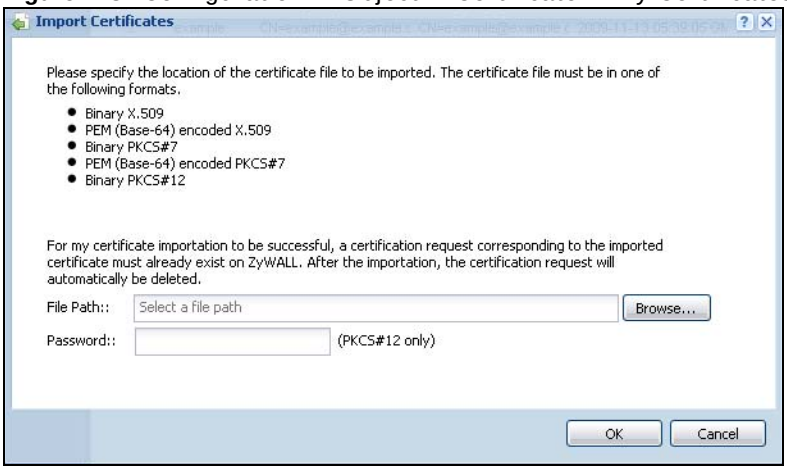
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyWALL.

Note: You can import a certificate that matches a corresponding certification request that was generated by the ZyWALL. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 278 Configuration > Object > Certificate > My Certificates > Import


Import Certificates
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
Binary PKCS#12
For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.
File Path::
Select a file path
Browse...
Password::
(PKCS#12 only)
OK
Cancel

The following table describes the labels in this screen.

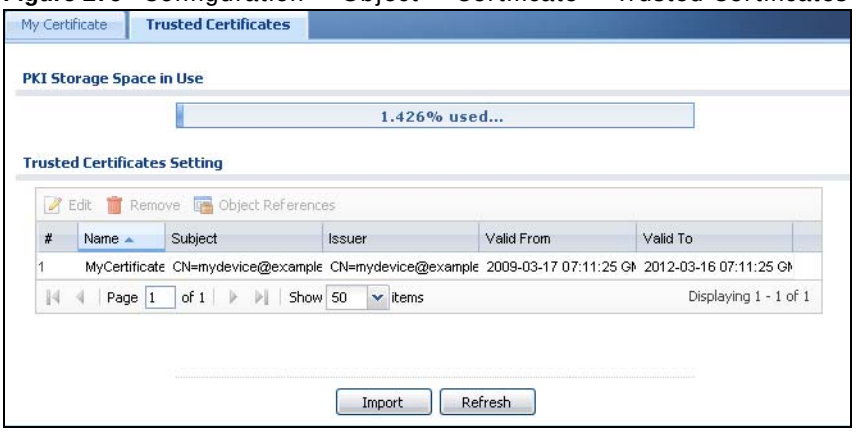
Table 162 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

33.3 The Trusted Certificates Screen

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the ZyWALL to accept as trusted. The ZyWALL also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 279 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 163 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.

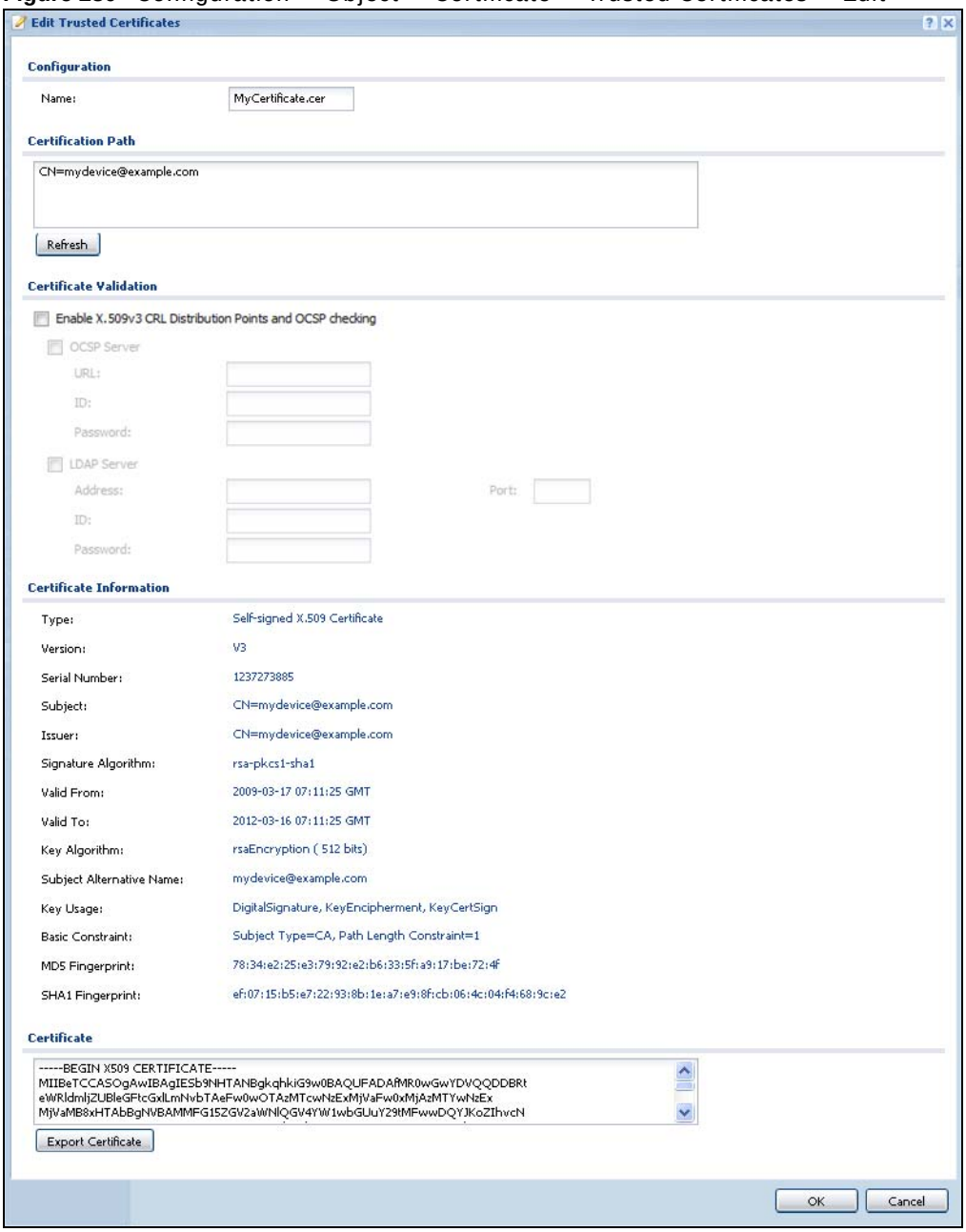
Table 163 Configuration > Object > Certificate > Trusted Certificates (continued)

LABEL	DESCRIPTION
Object References	You cannot delete certificates that any of the ZyWALL's features are configured to use. Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

33.3.1 The Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 280 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 164 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to turn on/off certificate revocation. When it is turned on, the ZyWALL validates a certificate by getting Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after selecting the **LDAP Server** check box) and online responder (can be configured after selecting the **OCSP Server** check box).
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and path name of the OCSP server.
ID	The ZyWALL may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The ZyWALL may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 164 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

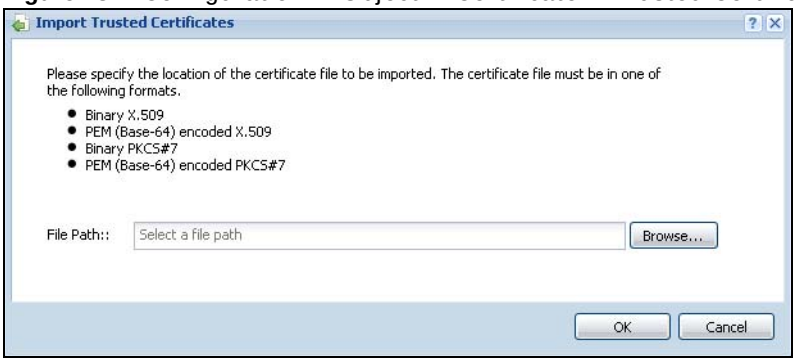
LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

33.3.2 The Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the ZyWALL.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 281 Configuration > Object > Certificate > Trusted Certificates > Import


Import Trusted Certificates
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path::
Select a file path
Browse...
OK
Cancel

The following table describes the labels in this screen.

Table 165 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the previous screen.

33.4 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the ZyWALL checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the ZyWALL only gets information on the certificates that it needs to verify, not a huge list. When the ZyWALL requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

34

ISP Accounts

34.1 Overview

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

Finding Out More

- See Section 7.4 on page 125 for information about PPPoE/PPTP interfaces.

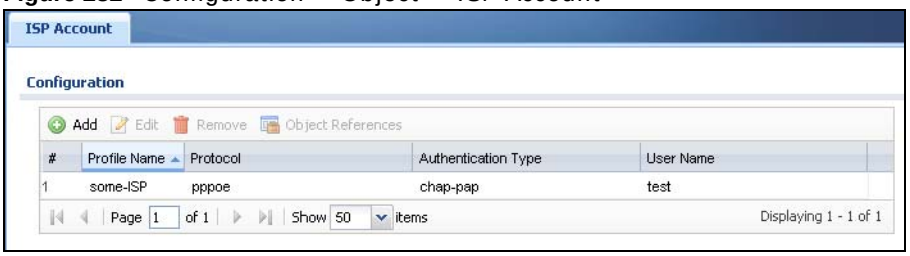
34.1.1 What You Can Do in this Chapter

Use the **Object** > **ISP Account** screens (Section 34.2 on page 429) to create and manage ISP accounts in the ZyWALL.

34.2 ISP Account Summary

This screen provides a summary of ISP accounts in the ZyWALL. To access this screen, click **Configuration > Object** > **ISP Account**.

Figure 282 Configuration > Object > ISP Account



The following table describes the labels in this screen. See the ISP Account Edit section below for more information as well.

Table 166 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific entry.

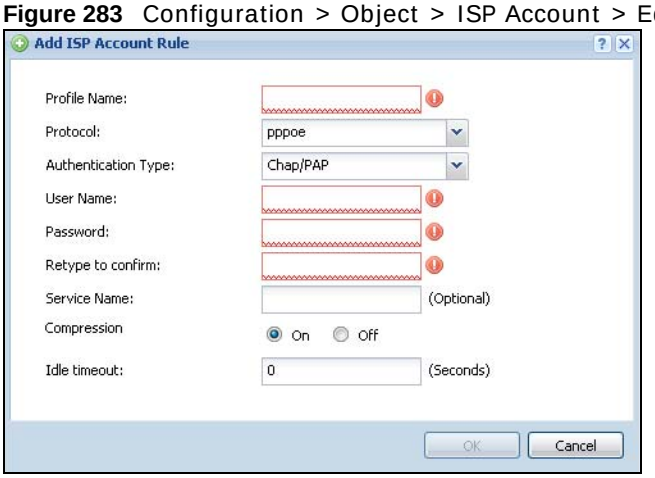
Table 166 Configuration > Object > ISP Account (continued)

LABEL	DESCRIPTION
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

34.2.1 ISP Account Edit

The **ISP Account Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See Section 34.2 on page 429.) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 283 Configuration > Object > ISP Account > Edit



The following table describes the labels in this screen.

Table 167 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: **pppoe** - This ISP account uses the PPPoE protocol. **pptp** - This ISP account uses the PPTP protocol.

Table 167 Configuration > Object > ISP Account > Edit (continued)

LABEL	DESCRIPTION
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **Chap** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only. **MSCHAP** - Your ZyWALL accepts MSCHAP only. **MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only.
Encryption Method	This field is available if this ISP account uses the **PPTP** protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **nomppe** - This ISP account does not use MPPE. **mppe-40** - This ISP account uses 40-bit MPPE. **mppe-128** - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the **PPTP** protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select **On** button to turn on stac compression, and select **Off** to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the ZyWALL automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click **OK** to save your changes back to the ZyWALL. If there are no errors, the program returns to the **ISP Account** screen. If there are errors, a message box explains the error, and the program stays in the **ISP Account Edit** screen.
Cancel	Click **Cancel** to return to the **ISP Account** screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

35

SSL Application

35.1 Overview

You use SSL application objects in SSL VPN. Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

35.1.1 What You Can Do in this Chapter

- Use the **SSL Application** screen (Section 35.2 on page 434) to view the ZyWALL's configured SSL application objects.
- Use the **SSL Application Edit** screen to create or edit web-based application objects to allow remote users to access an application via standard web browsers (Section 35.2.1 on page 435).
- You can also use the **SSL Application Edit** screen to specify the name of a folder on a Linux or Windows file server which remote users can access using a standard web browser (Section 35.2.1 on page 435).

35.1.2 What You Need to Know

Application Types

You can configure the following SSL application on the ZyWALL.

- Web-based

  A web-based application allows remote users to access an intranet site using standard web browsers.

Remote User Screen Links

Available SSL application names are displayed as links in remote user screens. Depending on the application type, remote users can simply click the links or follow the steps in the pop-up dialog box to access.

Remote Desktop Connections

Use SSL VPN to allow remote users to manage LAN computers. Depending on the functions supported by the remote desktop software, they can install or remove software, run programs, change settings, and open, copy, create, and delete files. This is useful for troubleshooting, support, administration, and remote access to files and programs.

The LAN computer to be managed must have VNC (Virtual Network Computing) or RDP (Remote Desktop Protocol) server software installed. The remote user's computer does not use VNC or RDP client software. The ZyWALL works with the following remote desktop connection software:

RDP

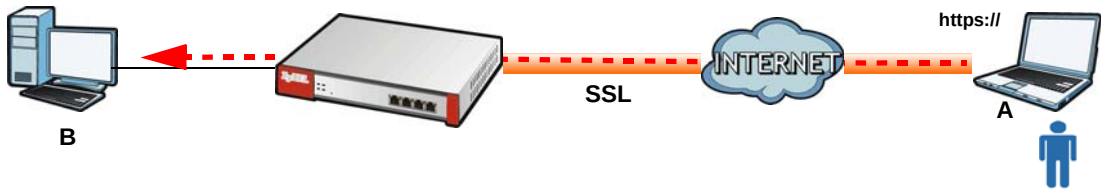
- Windows Remote Desktop (supported in Internet Explorer)

VNC

- RealVNC
- TightVNC
- UltraVNC

For example, user A uses an SSL VPN connection to log into the ZyWALL. Then he manages LAN computer B which has RealVNC server software installed.

Figure 284 SSL-protected Remote Management



Weblinks

You can configure weblink SSL applications to allow remote users to access web sites.

35.1.3 Example: Specifying a Web Site for Access

This example shows you how to create a web-based application for an internal web site. The address of the web site is http://info with web page encryption.

1 Click **Configuration > Object > SSL Application** in the navigation panel.

2 Click the **Add** button and select **Web Application** in the **Type** field.

In the **Server Type** field, select **Web Server**.

Enter a descriptive name in the **Display Name** field. For example, "CompanyIntranet".

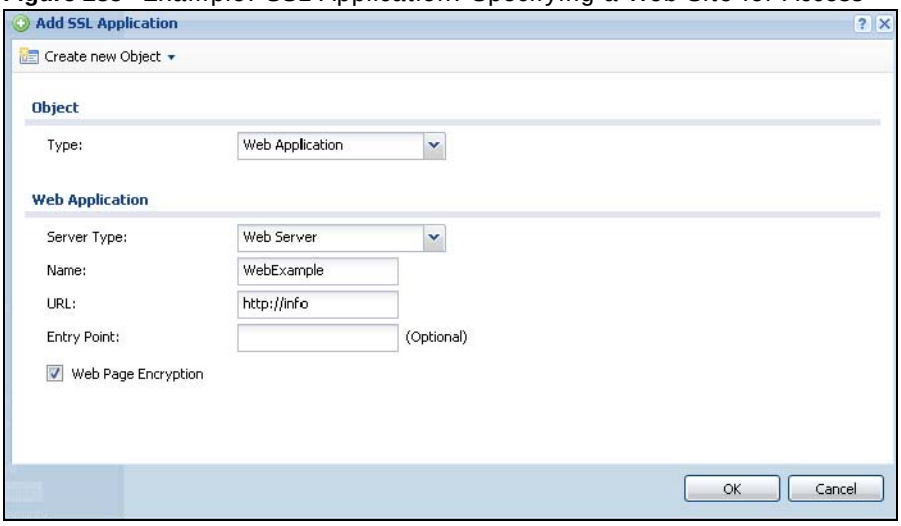
In the **Address** field, enter "http://info".

Select **Web Page Encryption** to prevent users from saving the web content.

Click **OK** to save the settings.

The configuration screen should look similar to the following figure.

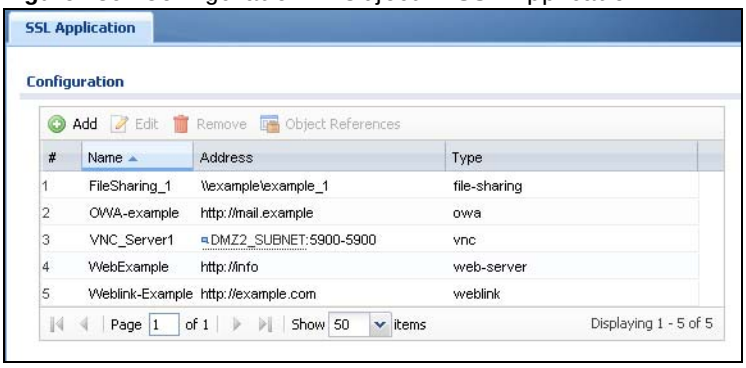
Figure 285 Example: SSL Application: Specifying a Web Site for Access



35.2 The SSL Application Screen

The main **SSL Application** screen displays a list of the configured SSL application objects. Click **Configuration > Object > SSL Application** in the navigation panel.

Figure 286 Configuration > Object > SSL Application



The following table describes the labels in this screen.

Table 168 Configuration > Object > SSL Application

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field displays the index number.
Name	This field displays the name of the object.

Table 168 Configuration > Object > SSL Application

LABEL	DESCRIPTION
Address	This field displays the IP address/URL of the application server or the location of a file share.
Type	This field shows whether the object is a file-sharing, web-server, Outlook Web Access, Virtual Network Computing, or Remote Desktop Protocol SSL application.

35.2.1 Creating/Editing an SSL Application Object

You can create a web-based application that allows remote users to access an application via standard web browsers. You can also create a file sharing application that specify the name of a folder on a file server (Linux or Windows) which remote users can access. Remote users can access files using a standard web browser and files are displayed as links on the screen.

To configure an SSL application, click the **Add** or **Edit** button in the **SSL Application** screen and select **Web Application** or **File Sharing** in the **Type** field. The screen differs depending on what object type you choose.

Note: If you are creating a file sharing SSL application, you must also configure the shared folder on the file server for remote access. Refer to the document that comes with your file server.

Figure 287 Configuration > Object > SSL Application > Add/Edit: Web Application

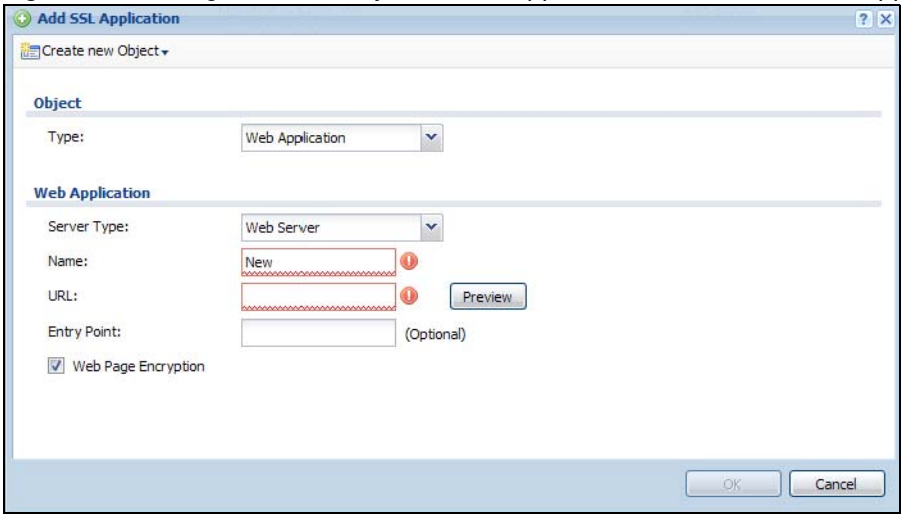
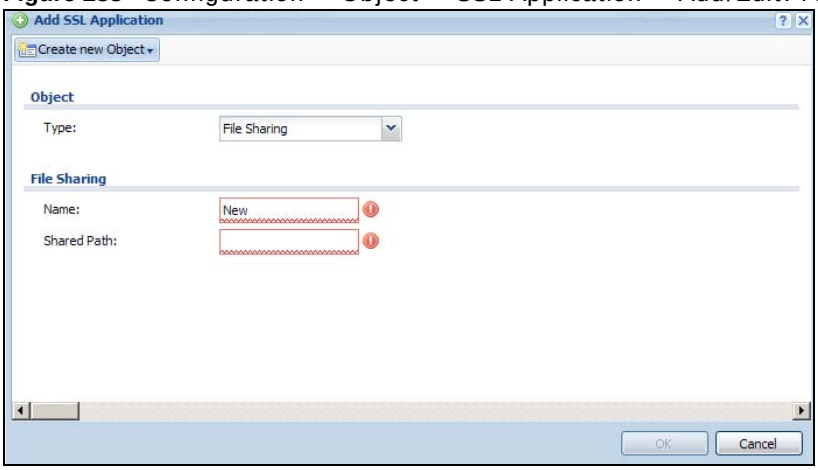


Figure 288 Configuration > Object > SSL Application > Add/Edit: File Sharing



The following table describes the labels in this screen.

Table 169 Configuration > Object > SSL Application > Add/Edit: Web Application

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Object	
Type	Select **Web Application** or **File Sharing** from the drop-down list box.
Web Application	
Server Type	This field only appears when you choose **Web Application** as the object type. Specify the type of service for this SSL application. Select **Web Server** to allow access to the specified web site hosted on the local network. Select **OWA** (Outlook Web Access) to allow users to access e-mails, contacts, calenders via Microsoft Outlook-like interface using supported web browsers. The ZyWALL supports one OWA object. Select **VNC** to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed. Select **RDP** to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed. Select **Weblink** to create a link to a web site that you expect the SSL VPN users to commonly use.
Name	Enter a descriptive name to identify this object. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). Spaces are not allowed.
URL	This field only appears when you choose **Web Application** as the object type. This field displays if the **Server Type** is set to **Web Server**, **OWA**, or **Weblink**. Enter the Fully-Qualified Domain Name (FQDN) or IP address of the application server. Note: You must enter the “http://” or “https://” prefix. Remote users are restricted to access only files in this directory. For example, if you enter “\remote\” in this field, remote users can only access files in the “remote” directory. If a link contains a file that is not within this domain, then remote users cannot access it.

Table 169 Configuration > Object > SSL Application > Add/Edit: Web Application (continued)

LABEL	DESCRIPTION
Preview	This field only appears when you choose **Web Application** as the object type. This field displays if the **Server Type** is set to **Web Server**, **OWA** or **Weblink**. Click **Preview** to access the URL you specified in a new IE web browser.
Entry Point	This field only appears when you choose **Web Application** as the object type. This field displays if the **Server Type** is set to **Web Server** or **OWA**. This field is optional. You only need to configure this field if you need to specify the name of the directory or file on the local server as the home page or home directory on the user screen.
Web Page Encryption	This field only appears when you choose **Web Application** as the object type. Select this option to prevent users from saving the web content.
Shared Path	This field only appears when you choose **File Sharing** as the object type. Specify the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats. "\\<IP address>\<share name>" "\\<domain name>\<share name>" "\\<computer name>\<share name>" For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer.
OK	Click **OK** to save the changes and return to the main **SSL Application Configuration** screen.
Cancel	Click **Cancel** to discard the changes and return to the main **SSL Application Configuration** screen.

36

DHCPv6

36.1 Overview

This chapter describes how to configure DHCPv6 request type and lease type objects.

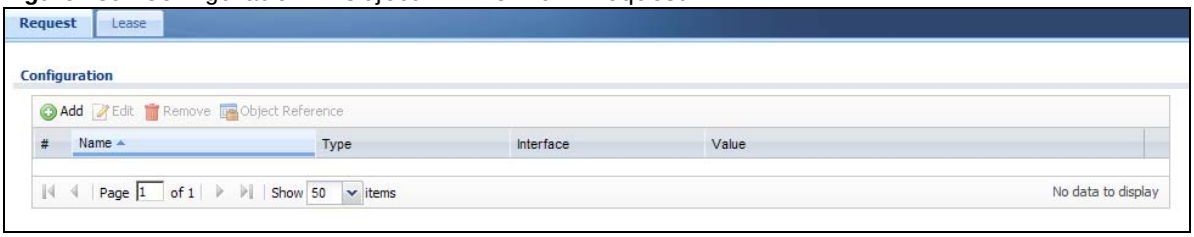
36.1.1 What You Can Do in this Chapter

- The **Request** screen (see Section 27.2 on page 373) allows you to configure DHCPv6 request type objects.
- The **Lease** screen (see Section 27.3 on page 376) allows you to configure DHCPv6 lease type objects.

36.2 The DHCPv6 Request Screen

The **Request** screen allows you to add, edit, and remove DHCPv6 request type objects. To access this screen, login to the Web Configurator, and click **Configuration > Object > DHCPv6 > Request**.

Figure 289 Configuration > Object > DHCPv6 > Request



The following table describes the labels in this screen.

Table 170 Configuration > Object > DHCPv6 > Request

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific object.
Name	This field displays the name of each request object.

Table 170 Configuration > Object > DHCPv6 > Request (continued)

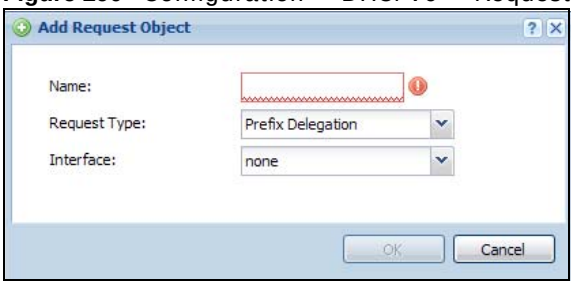
LABEL	DESCRIPTION
Type	This field displays the request type of each request object.
Interface	This field displays the interface used for each request object.
Value	This field displays the value for each request object.

36.2.1 DHCPv6 Request Add/Edit Screen

The **Request Add/Edit** screen allows you to create a new request object or edit an existing one.

To access this screen, go to the **Request** screen (see Section 27.2 on page 373), and click either the **Add** icon or an **Edit** icon.

Figure 290 Configuration > DHCPv6 > Request > Add



The following table describes the labels in this screen.

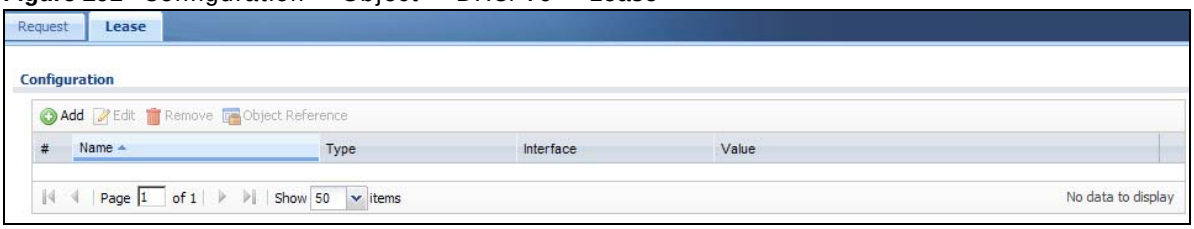
Table 171 Configuration > DHCPv6 > Request > Add

LABEL	DESCRIPTION
Name	Type the name for this request object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Request Type	Select the request type for this request object. You can choose from **Prefix Delegation**, **DNS Server**, **NTP Server**, or **SIP Server**.
Interface	Select the interface for this request object.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

36.3 The DHCPv6 Lease Screen

The **Lease** screen allows you to add, edit, and remove DHCPv6 lease type objects. To access this screen, login to the Web Configurator, and click **Configuration > Object > DHCPv6 > Lease**.

Figure 291 Configuration > Object > DHCPv6 > Lease



The following table describes the labels in this screen.

Table 172 Configuration > Object > DHCPv6 > Lease

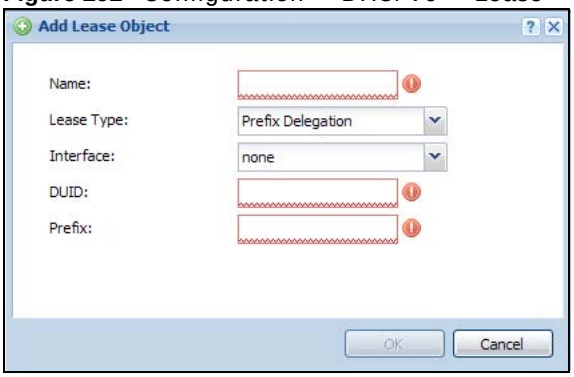
LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so.
Object References	Select an entry and click **Object Reference**s to open a screen that shows which settings use the entry. See Section 7.3.2 on page 122 for an example.
#	This field is a sequential value, and it is not associated with a specific object.
Name	This field displays the name of each lease object.
Type	This field displays the request type of each lease object.
Interface	This field displays the interface used for each lease object.
Value	This field displays the value for each lease object.

36.3.1 DHCPv6 Lease Add/Edit Screen

The **Lease Add / Edit** screen allows you to create a new lease object or edit an existing one.

To access this screen, go to the **Lease** screen (see Section 36.3 on page 439), and click either the **Add** icon or an **Edit** icon.

Figure 292 Configuration > DHCPv6 > Lease > Add



The following table describes the labels in this screen.

Table 173 Configuration > DHCPv6 > Lease > Add

LABEL	DESCRIPTION
Name	Type the name for this lease object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Lease Type	Select the lease type for this lease object. You can choose from **Prefix Delegation**, **DNS Server**, **Address**, **Address Pool**, **NTP Server**, or **SIP Server**.
Interface	Select the interface for this lease object.
DUID	If you select **Prefix Delegation** or **Address** in the **Lease Type field**, enter the DUID of the interface.
Prefix	If you select **Prefix Delegation** or **Address** in the **Lease Type field**, enter the IPv6 prefix of the interface.
DNS Server	If you select **DNS Server** in the **Lease Type field**, select a request object or **User Defined** in the **DNS Server** field and enter the IP address of the DNS server in the **User Defined Address** field below.
Starting IP Address	If you select **Address Pool** in the **Lease Type field**, enter the first of the contiguous addresses in the IP address pool.
End IP Address	If you select **Address Pool** in the **Lease Type field**, enter the last of the contiguous addresses in the IP address pool.
NTP Server	If you select **NTP Server** in the **Lease Type field**, select a request object or **User Defined** in the **NTP Server** field and enter the IP address of the NTP server in the **User Defined Address** field below.
SIP Server	If you select **SIP Server** in the **Lease Type field**, select a request object or **User Defined** in the **SIP** field and enter the IP address of the SIP server in the **User Defined Address** field below.
User Defined Address	If you select **DNS Server**, **NTP Server**, or **SIP Server** as your lease type, you must enter the IP address of the server your selected.
OK	Click **OK** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving your changes.

37

System

37.1 Overview

Use the system screens to configure general ZyWALL settings.

37.1.1 What You Can Do in this Chapter

- Use the **System > Host Name** screen (see Section 37.2 on page 444) to configure a unique name for the ZyWALL in your network.
- Use the **System > USB Storage** screen (see Section 37.3 on page 444) to configure the settings for the connected USB devices.
- Use the **System > Date/Time** screen (see Section 37.4 on page 445) to configure the date and time for the ZyWALL.
- Use the **System > Console Speed** screen (see Section 37.5 on page 449) to configure the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program.
- Use the **System > DNS** screen (see Section 37.6 on page 450) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the **System > WWW** screens (see Section 37.7 on page 456) to configure settings for HTTP or HTTPS access to the ZyWALL and how the login and access user screens look.
- Use the **System > SSH** screen (see Section 37.8 on page 472) to configure SSH (Secure SHell) used to securely access the ZyWALL's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the **System > TELNET** screen (see Section 37.9 on page 476) to configure Telnet to access the ZyWALL's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the **System > FTP** screen (see Section 37.10 on page 478) to specify from which zones FTP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come. You can upload and download the ZyWALL's firmware and configuration files using FTP. Please also see Chapter 39 on page 499 for more information about firmware and configuration files.
- Your ZyWALL can act as an SNMP agent, which allows a manager station to manage and monitor the ZyWALL through the network. Use the **System > SNMP** screen (see Section 37.11 on page 479) to configure SNMP settings, including from which zones SNMP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.
- Use the **System > Language** screen (see Section 37.12 on page 483) to set a language for the ZyWALL's Web Configurator screens.
- Use the **System > IPv6** screen (see Section 37.13 on page 483) to enable or disable IPv6 support on the ZyWALL.

Note: See each section for related background information and term definitions.

37.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open the **Host Name** screen.

Figure 293 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 174 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Enter a descriptive name to identify your ZyWALL device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

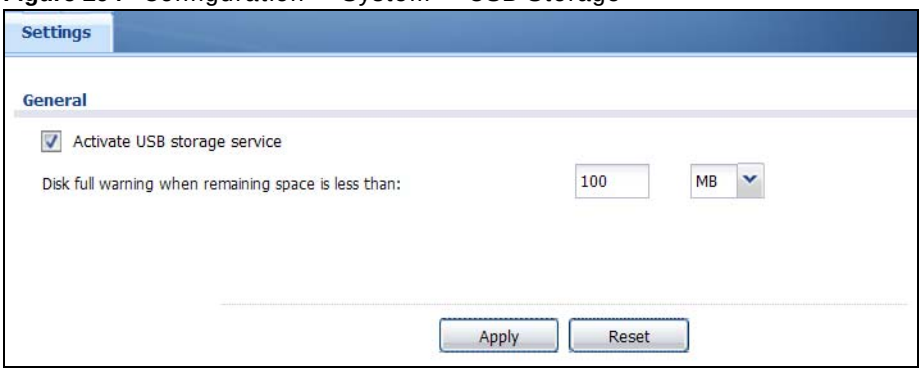
37.3 USB Storage

The ZyWALL can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

Click **Configuration > System > USB Storage** to open the screen as shown next.

Figure 294 Configuration > System > USB Storage



The following table describes the labels in this screen.

Table 175 Configuration > System > USB Storage

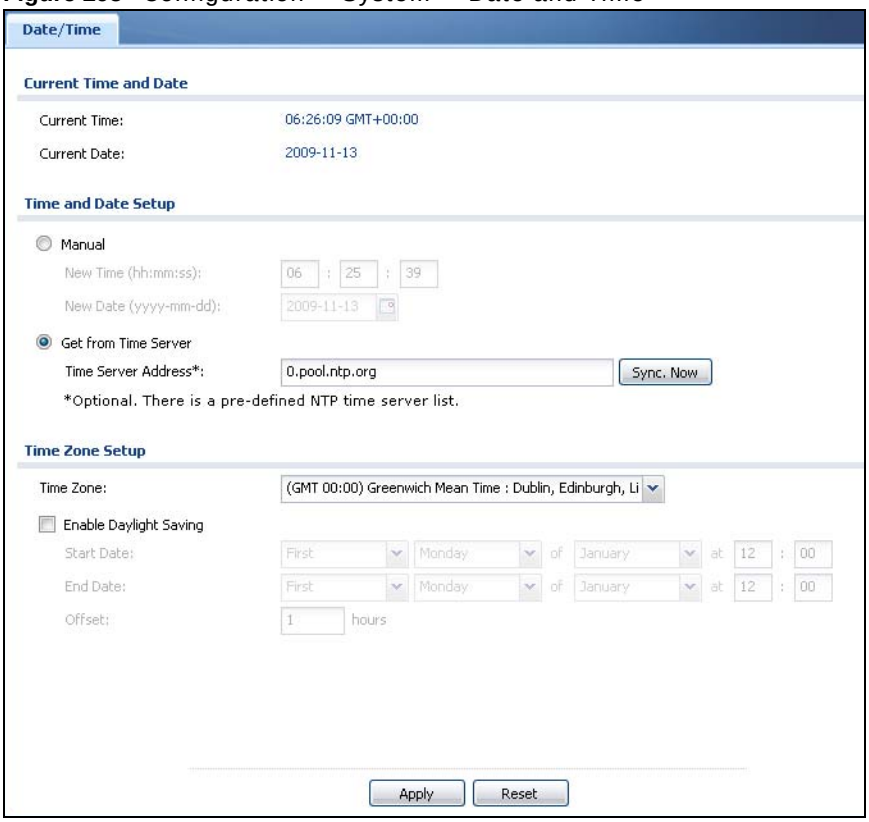
LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (**MB** or **%**) to have the ZyWALL send a warning message when the remaining USB storage space is less than the value you set here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.4 Date and Time

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your ZyWALL's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the ZyWALL's time and date or have the ZyWALL get the date and time from a time server.

Figure 295 Configuration > System > Date and Time



The following table describes the labels in this screen.

Table 176 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your ZyWALL.
Current Date	This field displays the present date of your ZyWALL.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the ZyWALL uses the new setting once you click **Apply**.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.

Table 176 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the ZyWALL get the time and date from the time server you specify below. The ZyWALL requests time and date settings from the time server under the following circumstances. • When the ZyWALL starts up. • When you click **Apply** or **Synchronize Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the ZyWALL get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.4.1 Pre-defined NTP Time Servers List

When you turn on the ZyWALL for the first time, the date and time start at 2003-01-01 00:00:00. The ZyWALL then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The ZyWALL continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 177 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

When the ZyWALL uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

37.4.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Please Wait...** screen appears, you may have to wait up to one minute.

Figure 296 Synchronization in Process



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the ZyWALL date and time.

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the ZyWALL's time in the **New Time** field.

4 Enter the ZyWALL's date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.

7 Click **Apply**.

To get the ZyWALL date and time from a time server

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

4 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.

5 Under **Time and Date Setup**, enter a **Time Server Address** (Table 177 on page 448).

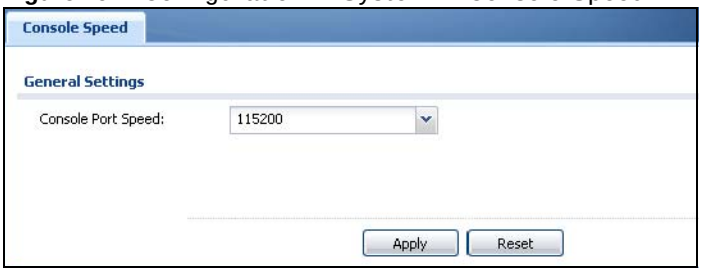
6 Click **Apply**.

37.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program. See Table 2 on page 20 for default console port settings.

Click **Configuration > System > Console Speed** to open the **Console Speed** screen.

Figure 297 Configuration > System > Console Speed



The following table describes the labels in this screen.

Table 178 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your ZyWALL supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The **Console Port Speed** applies to a console port connection using terminal emulation software and NOT the **Console** in the ZyWALL Web Configurator **Status** screen.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

37.6.1 DNS Server Address Assignment

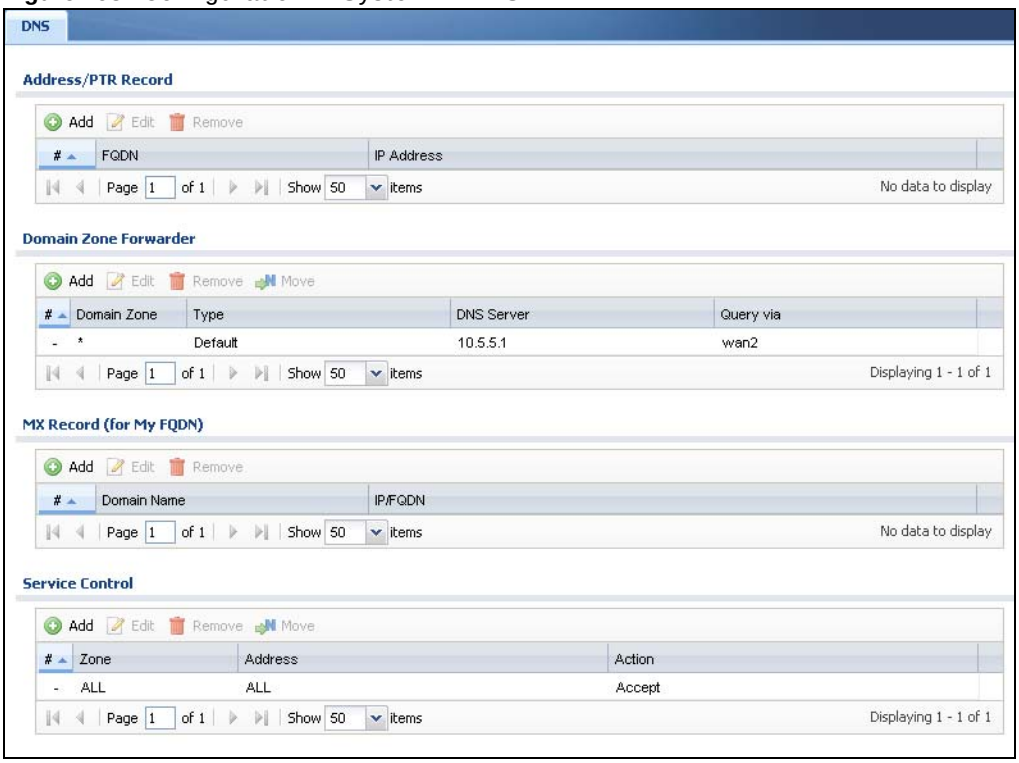
The ZyWALL can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

37.6.2 Configuring the DNS Screen

Click **Configuration > System > DNS** to change your ZyWALL's DNS settings. Use the **DNS** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server. You can also configure the ZyWALL to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the ZyWALL sends to the specified DHCP client devices.

Figure 298 Configuration > System > DNS



The following table describes the labels in this screen.

Table 179 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host’s fully qualified domain name.
IP Address	This is the IP address of a host.
Domain Zone Forwarder	This specifies a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the ZyWALL needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry’s position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The ZyWALL uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A “*” means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (**User-Defined**).
DNS Server	This is the IP address of a DNS server. This field displays **N/A** if you have the ZyWALL get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the ZyWALL sends DNS queries to the entry’s DNS server. If the ZyWALL connects through a VPN tunnel, **tunnel** displays.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry’s settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.

Table 179 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Service Control	This specifies from which computers and zones you can send DNS queries to the ZyWALL.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the ZyWALL accepts DNS queries from the computer with the IP address specified above through the specified zone (**Accept**) or discards them (**Deny**).

37.6.3 Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

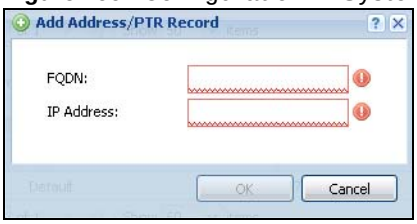
37.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

37.6.5 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

Figure 299 Configuration > System > DNS > Address/PTR Record Edit



The following table describes the labels in this screen.

Table 180 Configuration > System > DNS > Address/PTR Record Edit

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

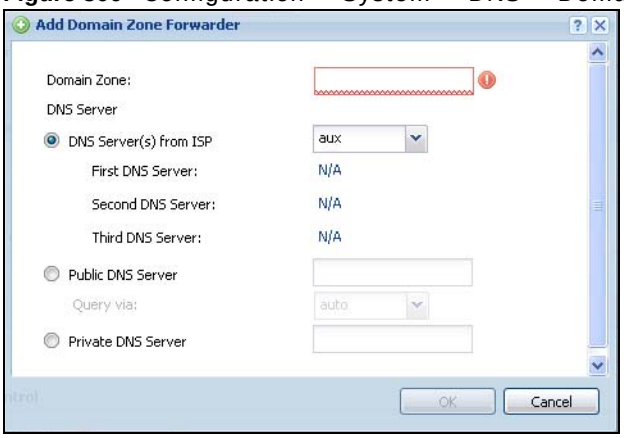
37.6.6 Domain Zone Forwarder

A domain zone forwarder contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

37.6.7 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

Figure 300 Configuration > System > DNS > Domain Zone Forwarder Add



The following table describes the labels in this screen.

Table 181 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select **DNS Server(s) from ISP** if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select **Public DNS Server** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The ZyWALL must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the ZyWALL's local networks. You cannot use 0.0.0.0. Use the **Query via** field to select the interface through which the ZyWALL sends DNS queries to a DNS server. Select **Private DNS Server** if you have the IP address of a DNS server to which the ZyWALL connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

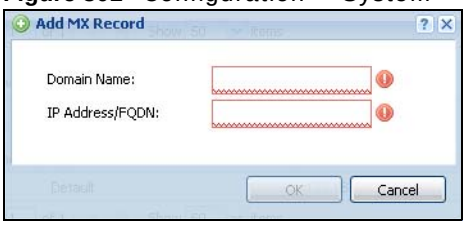
37.6.8 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

37.6.9 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 301 Configuration > System > DNS > MX Record Add



The following table describes the labels in this screen.

Table 182 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

37.6.10 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

Figure 302 Configuration > System > DNS > Service Control Rule Add



The following table describes the labels in this screen.

Table 183 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to send DNS queries to the ZyWALL. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the ZyWALL.
Zone	Select **ALL** to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the ZyWALL is allowed or denied.
Action	Select **Accept** to have the ZyWALL allow the DNS queries from the specified computer. Select **Deny** to have the ZyWALL reject the DNS queries from the specified computer.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

37.7 WWW Overview

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Note: To allow the ZyWALL to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ZyWALL firewall rule to block that traffic.

- See To-ZyWALL Rules on page 266 for more on To-ZyWALL firewall rules.

To stop a service from accessing the ZyWALL, clear **Enable** in the corresponding service screen.

37.7.1 Service Access Limitations

A service cannot be used to access the ZyWALL when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the ZyWALL disallows the session).
3. The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
4. There is a firewall rule that blocks it.

37.7.2 System Timeout

There is a lease timeout for administrators. The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User / Group** screens.

37.7.3 HTTPS

You can set the ZyWALL to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 33 on page 413 for more information).

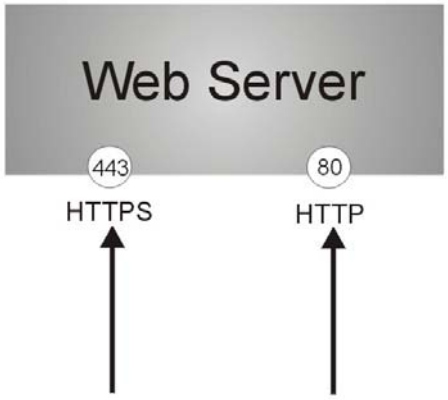
HTTPS on the ZyWALL is used so that you can securely access the ZyWALL using the Web Configurator. The SSL protocol specifies that the HTTPS server (the ZyWALL) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the ZyWALL), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's web server.

Figure 303 HTTP/HTTPS Implementation



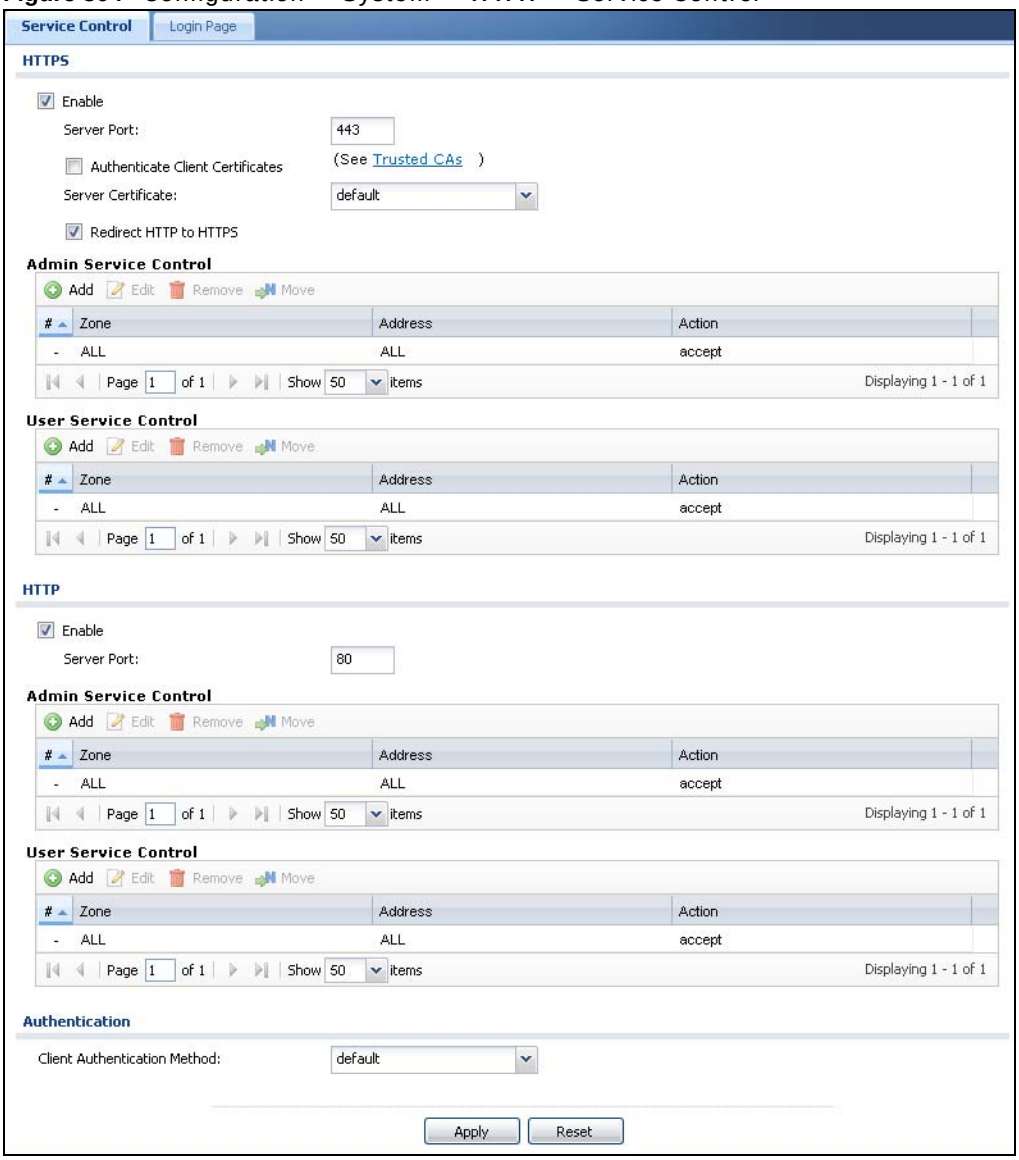
Note: If you disable **HTTP** in the **WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

37.7.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the ZyWALL using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: **Admin Service Control** deals with management access (to the Web Configurator). **User Service Control** deals with user access to the ZyWALL (logging into SSL VPN for example).

Figure 304 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 184 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL Web Configurator to use "https://ZyWALL IP Address:**8443**" as the URL.

Table 184 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Section 37.7.7.5 on page 467 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the ZyWALL) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTPS to manage the ZyWALL (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL. **User Service Control** specifies from which zones a user can use HTTPS to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the ZyWALL.
Admin/User Service Control	**Admin Service Control** specifies from which zones an administrator can use HTTP to manage the ZyWALL (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL. **User Service Control** specifies from which zones a user can use HTTP to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

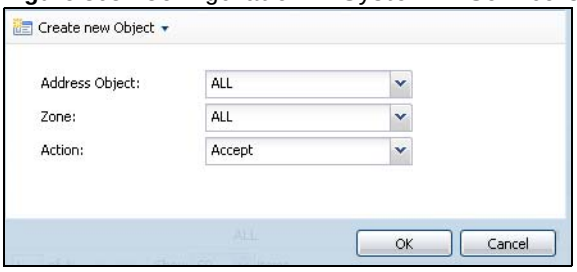
Table 184 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the **Auth. method** screen.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.7.5 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

Figure 305 Configuration > System > Service Control Rule > Edit



The following table describes the labels in this screen.

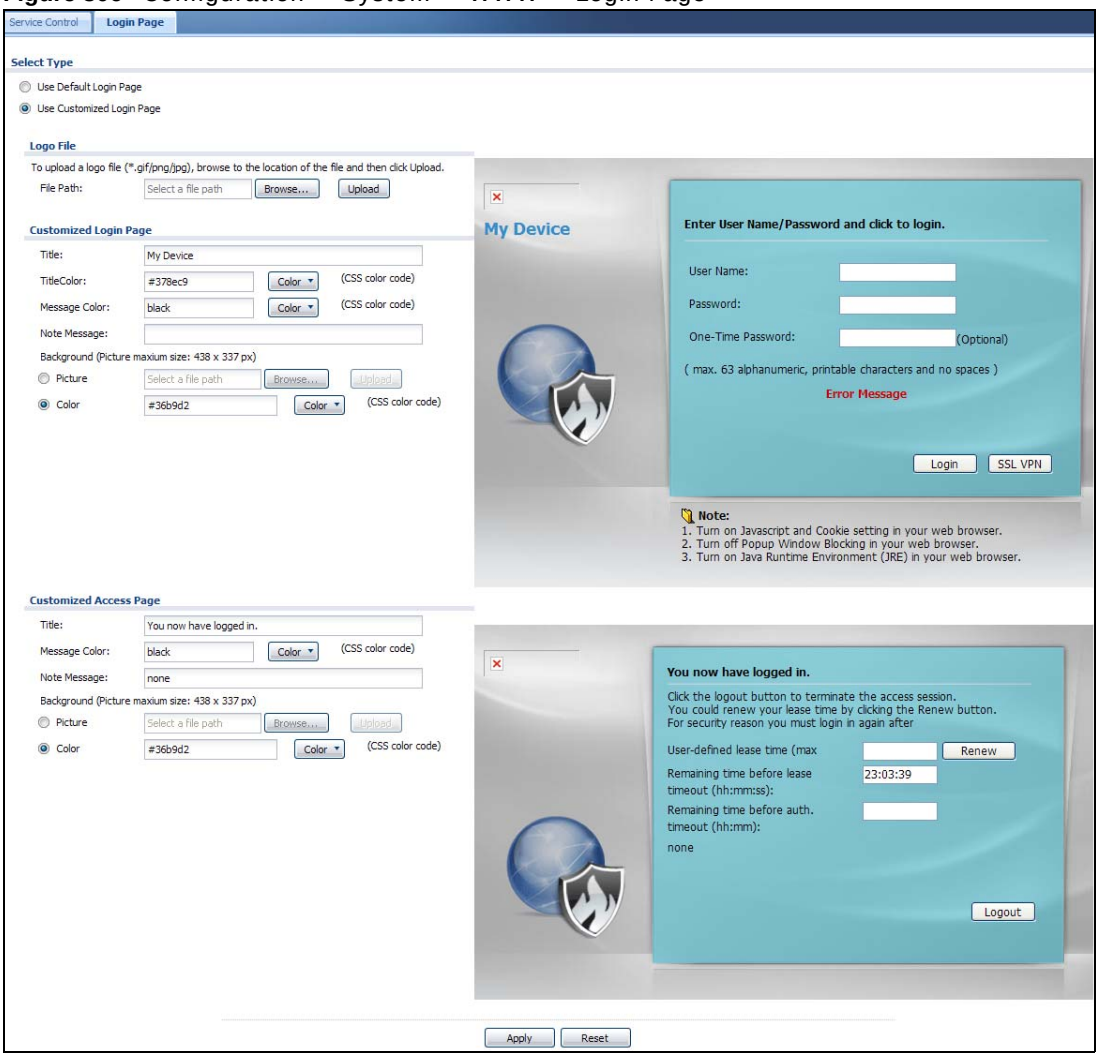
Table 185 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select **ALL** to allow or deny any computer to communicate with the ZyWALL using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the ZyWALL using this service.
Zone	Select **ALL** to allow or prevent any ZyWALL zones from being accessed using this service. Select a predefined ZyWALL zone on which a incoming service is allowed or denied.
Action	Select **Accept** to allow the user to access the ZyWALL from the specified computers. Select **Deny** to block the user's access to the ZyWALL from the specified computers.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving

37.7.6 Customizing the WWW Login Page

Click **Configuration > System > WWW > Login Page** to open the **Login Page** screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See Chapter 27 on page 371 for more on access user accounts.

Figure 306 Configuration > System > WWW > Login Page



The following figures identify the parts you can customize in the login and access pages.

Figure 307 Login Page Customization

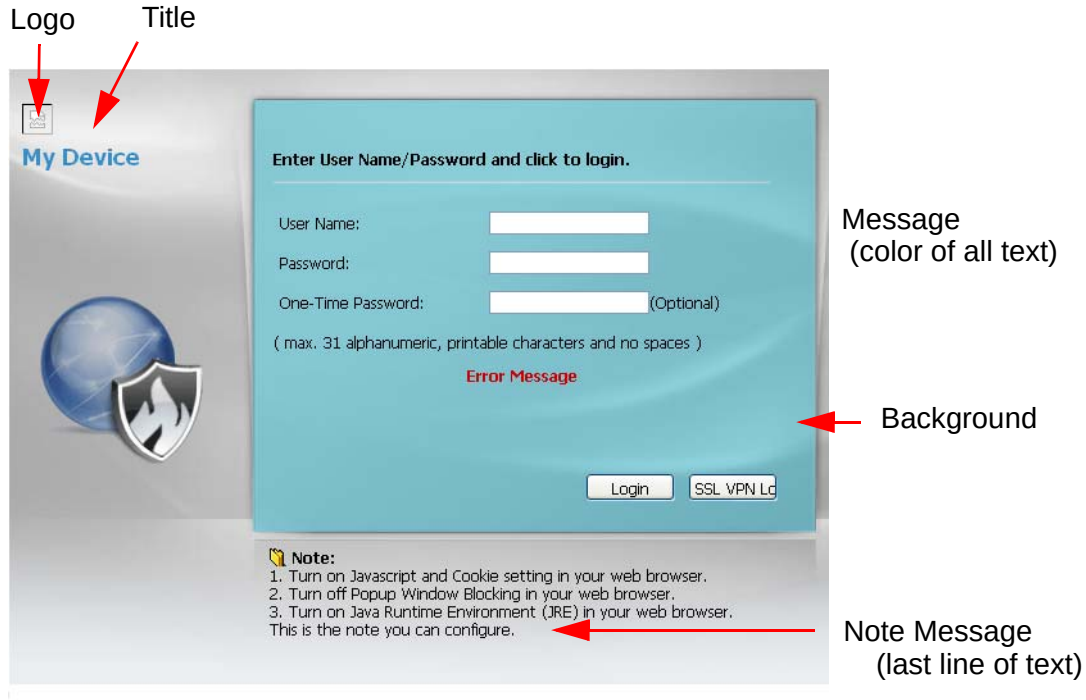
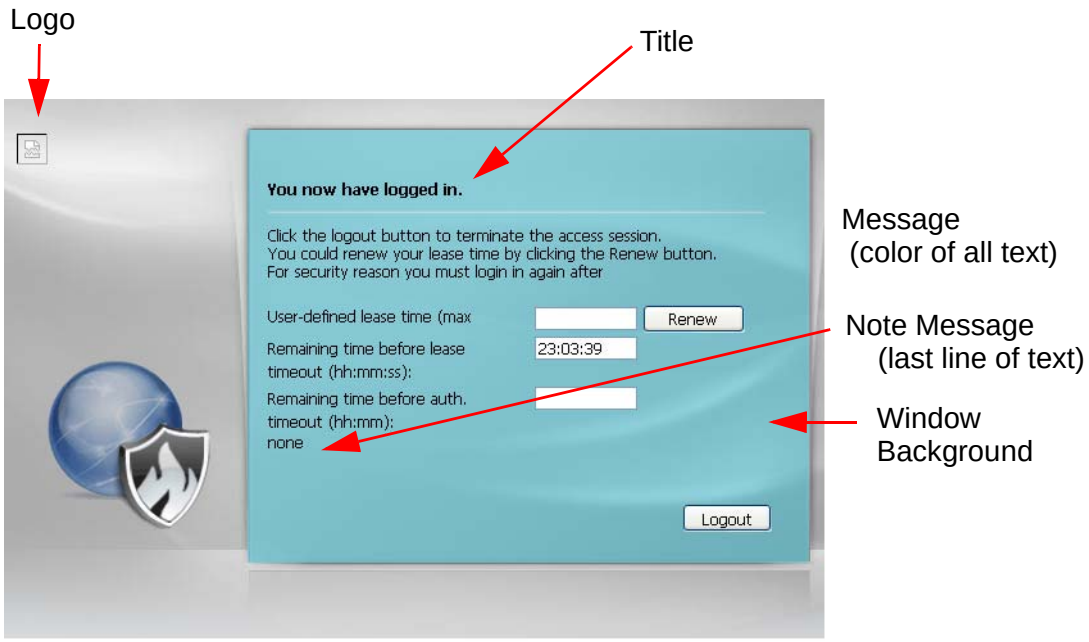


Figure 308 Access Page Customization



You can specify colors in one of the following ways:

- Click **Color** to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.

- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.
- Enter "rgb" followed by red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.

Your desired color should display in the preview screen on the right after you click in another field, click **Apply**, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

Table 186 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click **Browse** to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click **Upload** to transfer the specified graphic file from your computer to the ZyWALL.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed.

Table 186 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Background	Set how the window's background looks. To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select **Color** and specify the color.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

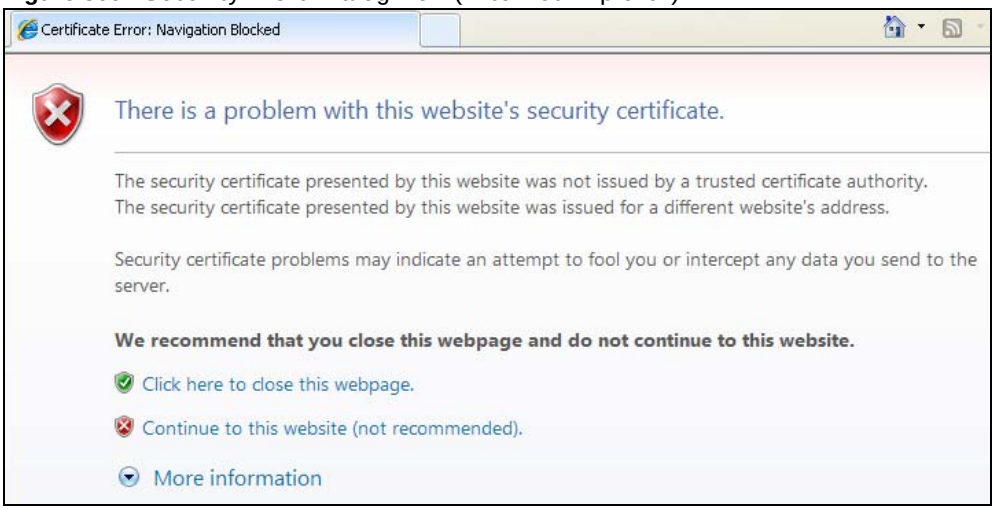
37.7.7 HTTPS Example

If you haven't changed the default HTTPS port on the ZyWALL, then in your browser enter "https://ZyWALL IP Address/" as the web site address where "ZyWALL IP Address" is the IP address or domain name of the ZyWALL you wish to access.

37.7.7.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, you will see the error message shown in the following screen.

Figure 309 Security Alert Dialog Box (Internet Explorer)


Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Select **Continue to this website** to proceed to the Web Configurator login screen. Otherwise, select **Click here to close this webpage** to block the access.

37.7.7.2 Mozilla Firefox Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **The Connection is Untrusted** screen appears as shown in the following screen. Click **Technical Details** if you want to verify more information about the certificate from the ZyWALL.

Select **I Understand the Risks** and then click **Add Exception** to add the ZyWALL to the security exception list. Click **Confirm Security Exception**.

Figure 310 Security Certificate 1 (Firefox)

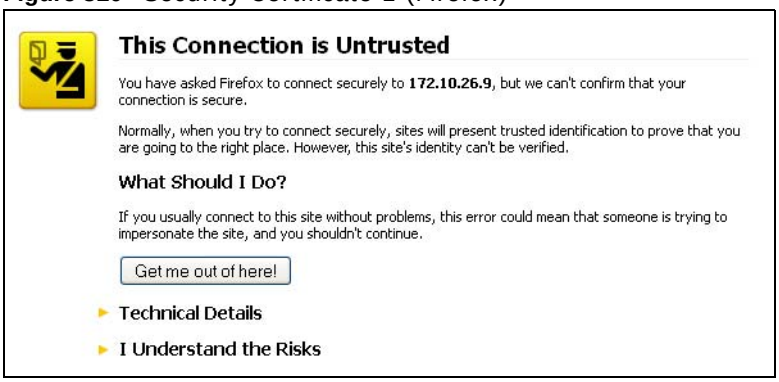
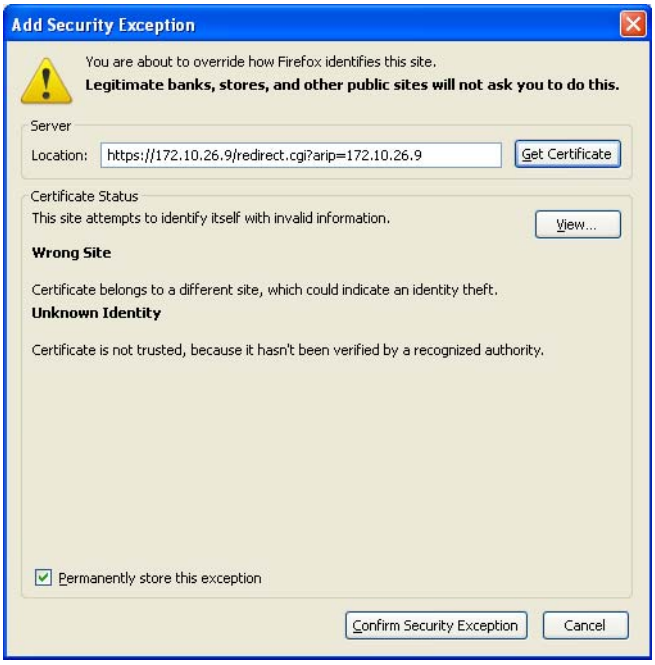

This Connection is Untrusted
You have asked Firefox to connect securely to 172.10.26.9, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

Figure 311 Security Certificate 2 (Firefox)


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://172.10.26.9/redirect.cgi?arip=172.10.26.9
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

37.7.7.3 Avoiding Browser Warning Messages

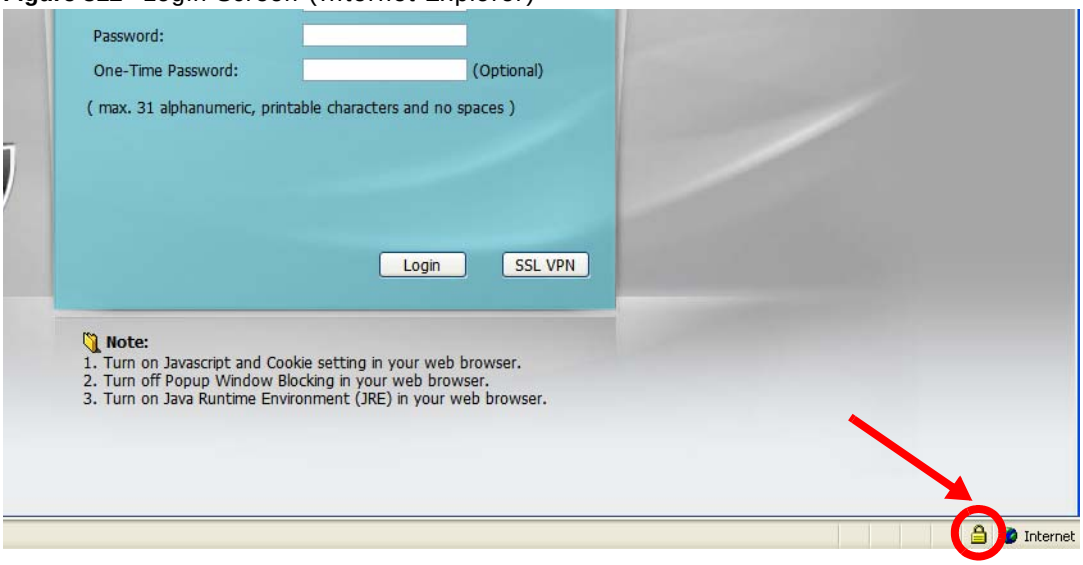
Here are the main reasons your browser displays warnings about the ZyWALL's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the ZyWALL's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.

37.7.7.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 312 Login Screen (Internet Explorer)


Password:
One-Time Password:
(Optional)
(max. 31 alphanumeric, printable characters and no spaces)
Login
SSL VPN
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
Internet

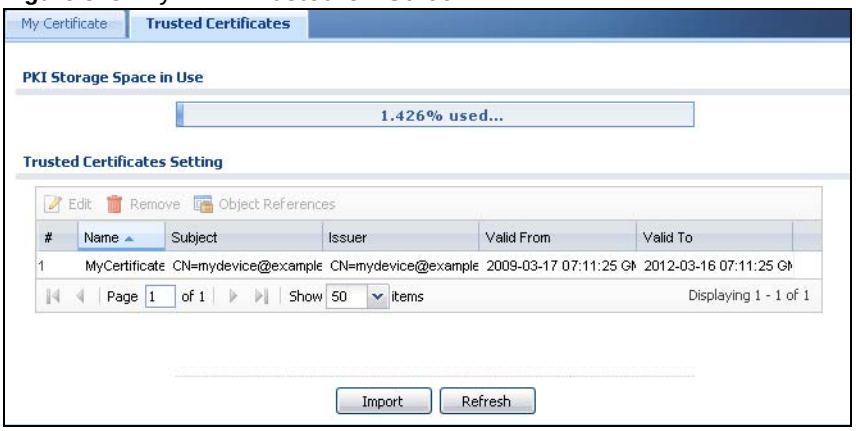
37.7.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** Web Configurator screen).

Figure 313 ZyWALL Trusted CA Screen



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

37.7.7.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 314 CA Certificate Example



2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

37.7.7.5.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

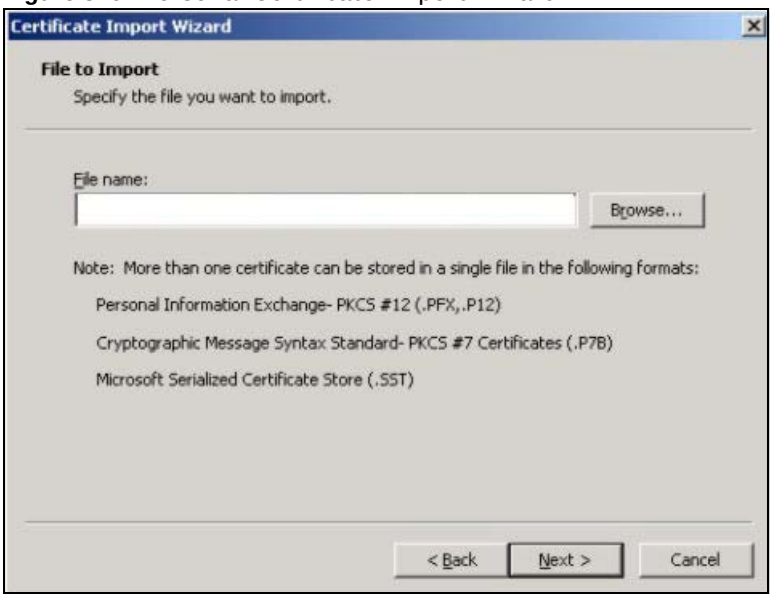
1 Click **Next** to begin the wizard.

Figure 315 Personal Certificate Import Wizard 1


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 316 Personal Certificate Import Wizard 2


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

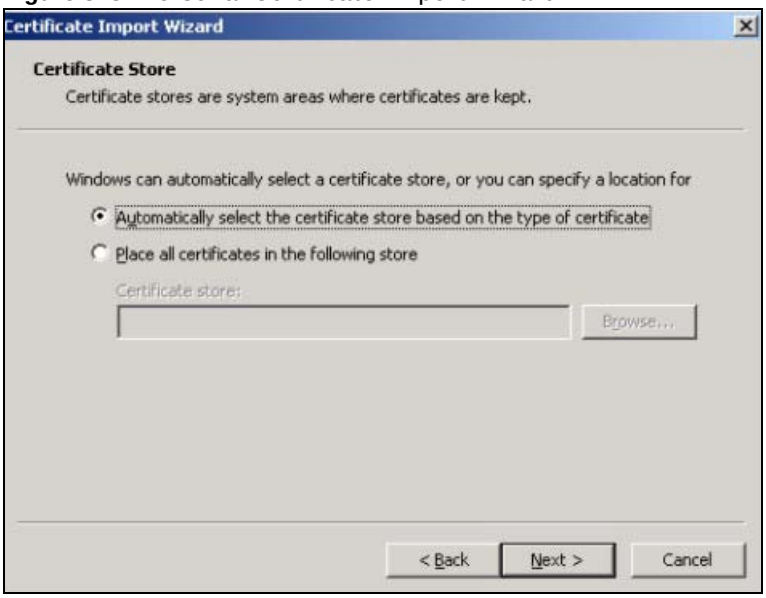
3 Enter the password given to you by the CA.

Figure 317 Personal Certificate Import Wizard 3


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark the private key as exportable
< Back
Next >
Cancel

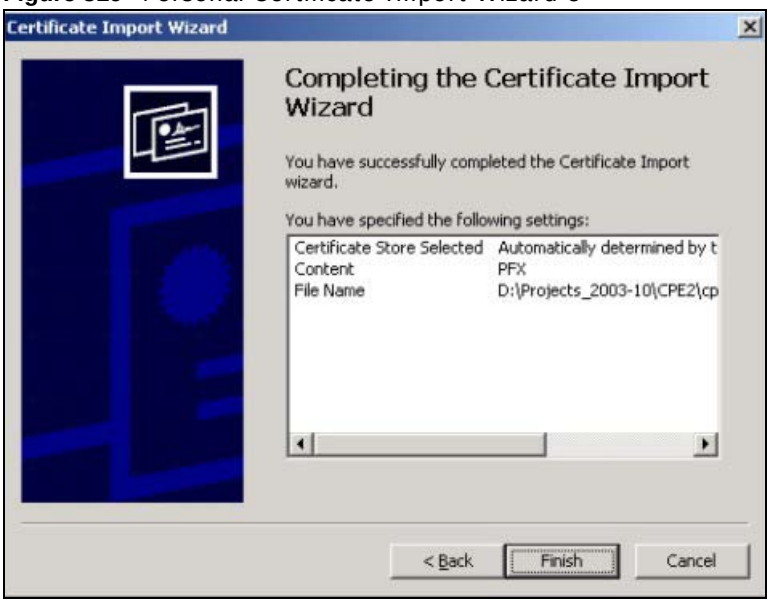
4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 318 Personal Certificate Import Wizard 4


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

5 Click **Finish** to complete the wizard and begin the import process.

Figure 319 Personal Certificate Import Wizard 5



6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 320 Personal Certificate Import Wizard 6



37.7.7.6 Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

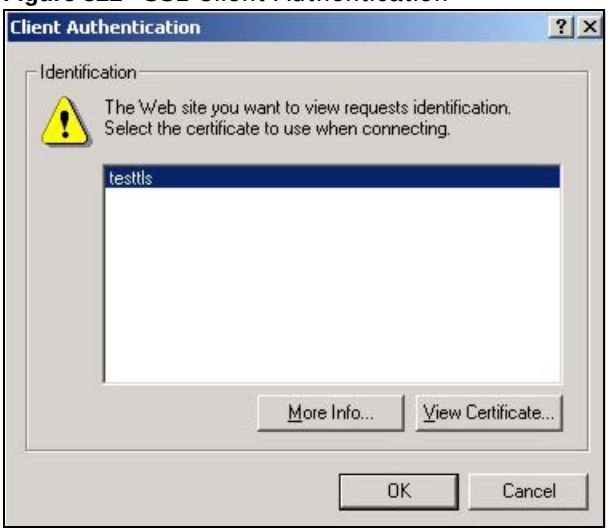
1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

Figure 321 Access the ZyWALL Via HTTPS



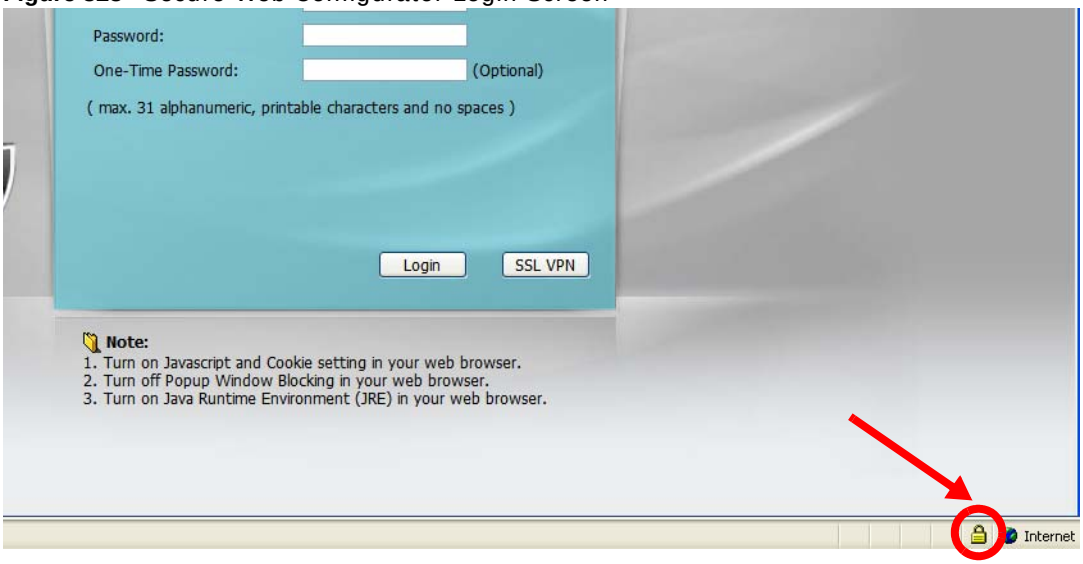
2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

Figure 322 SSL Client Authentication



3 You next see the Web Configurator login screen.

Figure 323 Secure Web Configurator Login Screen


Password:
One-Time Password:
(Optional)
(max. 31 alphanumeric, printable characters and no spaces)
Login
SSL VPN
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
Internet

37.8 SSH

You can use SSH (Secure SHell) to securely access the ZyWALL's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the ZyWALL for a management session.

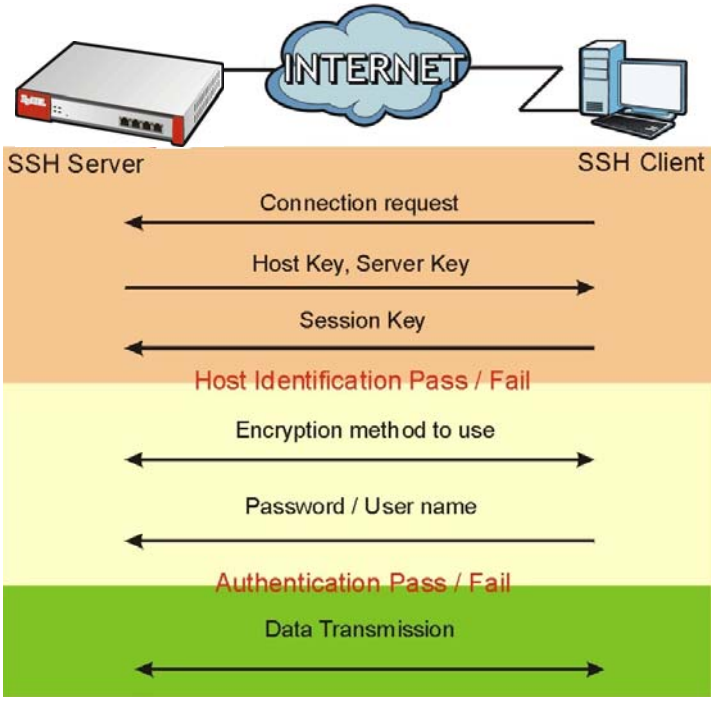
Figure 324 SSH Communication Over the WAN Example



37.8.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 325 How SSH v1 Works Example



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

37.8.2 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ZyWALL for management using port 22 (by default).

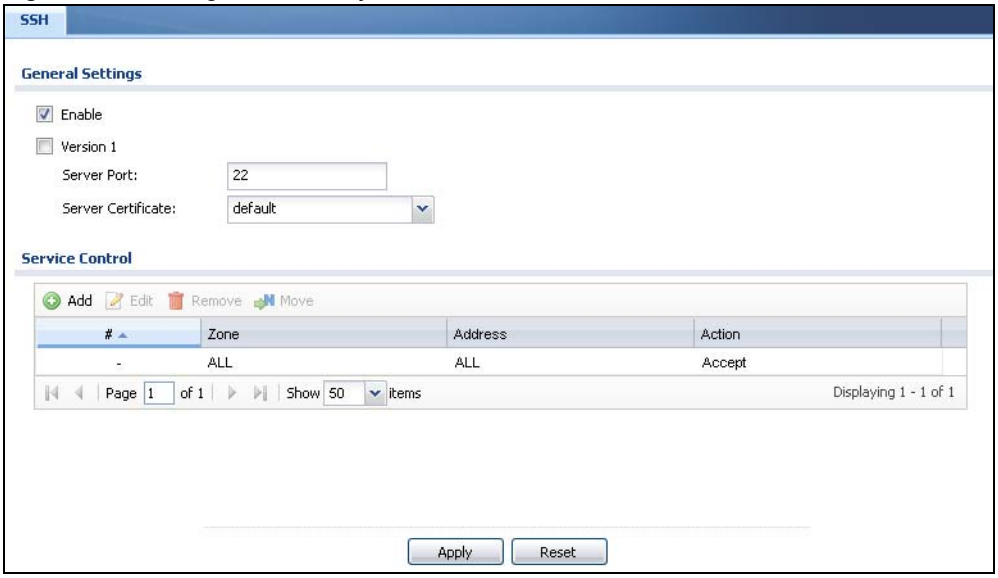
37.8.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

37.8.4 Configuring SSH

Click **Configuration > System > SSH** to change your ZyWALL's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 326 Configuration > System > SSH



The following table describes the labels in this screen.

Table 187 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service.
Version 1	Select the check box to have the ZyWALL use both SSH version 1 and version 2 protocols. If you clear the check box, the ZyWALL uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 33 on page 413 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.

Table 187 Configuration > System > SSH (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 185 on page 461 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.8.5 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

37.8.5.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number) for the ZyWALL.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 327 SSH Example 1: Store Host Key


Host Identification
You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.
The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"
You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.
Do you want to save the new host key to the local database?
Yes
No
Cancel
Help

Enter the password to log in to the ZyWALL. The CLI screen displays next.

37.8.5.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ZyWALL.

Enter "telnet 192.168.1.1 22" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ZyWALL.

Figure 328 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "ssh –1 192.168.1.1". This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "yes" and press [ENTER].

Then enter the password to log in to the ZyWALL.

Figure 329 SSH Example 2: Log in

```
$ ssh –1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

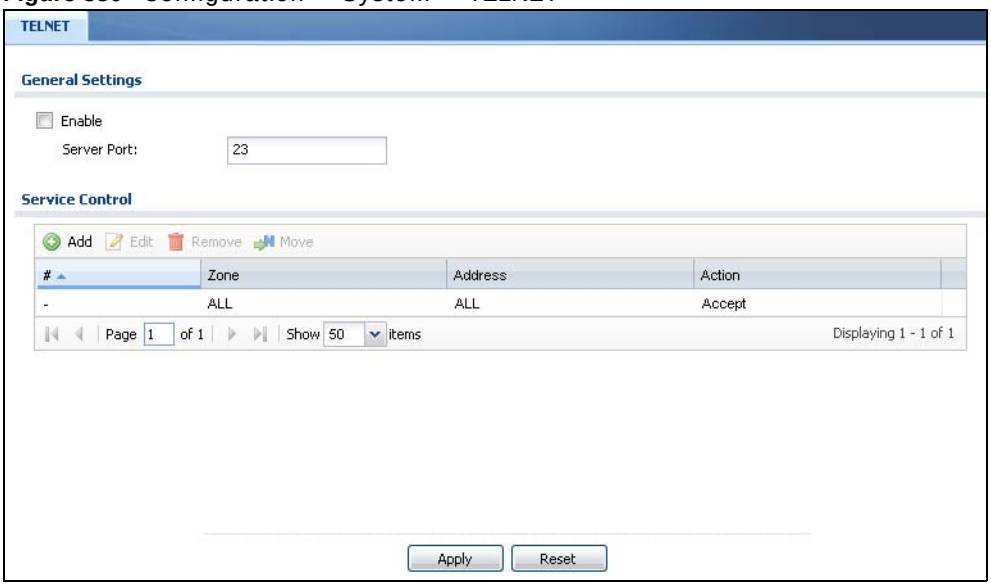
37.9 Telnet

You can use Telnet to access the ZyWALL's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

37.9.1 Configuring Telnet

Click **Configuration > System > TELNET** to configure your ZyWALL for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 330 Configuration > System > TELNET



The following table describes the labels in this screen.

Table 188 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which ZyWALL zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 185 on page 461 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

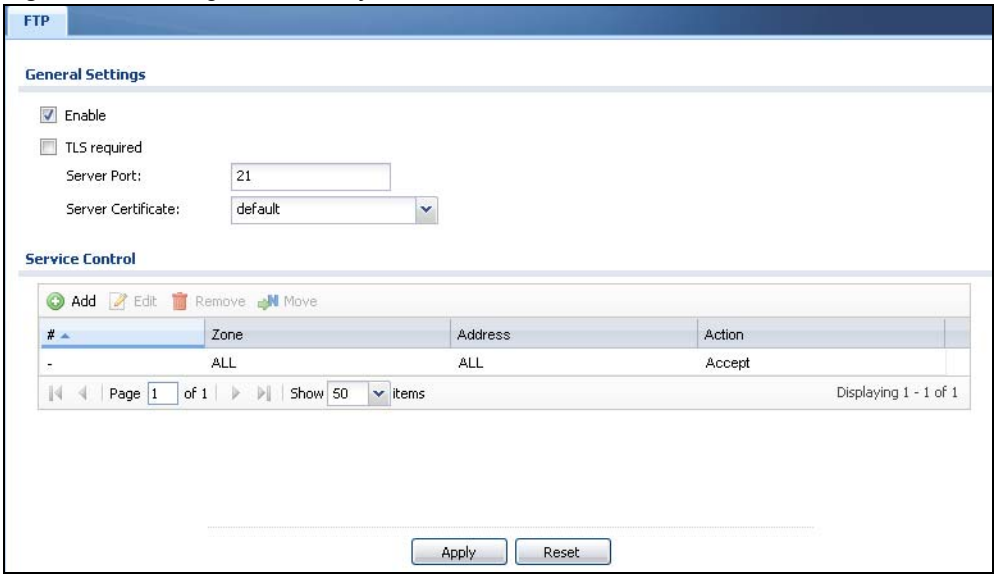
37.10 FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see Chapter 39 on page 499 for more information about firmware and configuration files.

37.10.1 Configuring FTP

To change your ZyWALL's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 331 Configuration > System > FTP



The following table describes the labels in this screen.

Table 189 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for FTP connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 33 on page 413 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 185 on page 461 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.

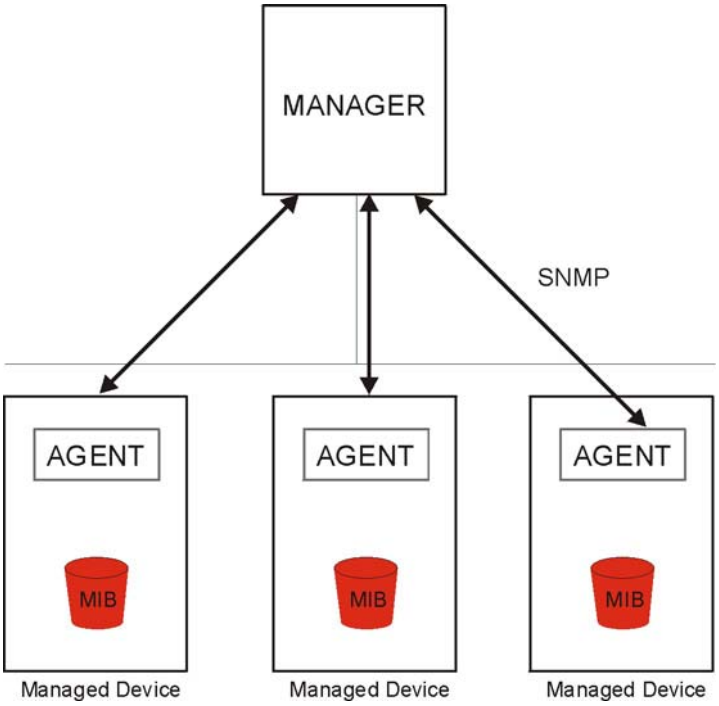
Table 189 Configuration > System > FTP (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 332 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

37.11.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect

statistical data and monitor status and performance. You can download the ZyWALL's MIBs from www.zyxel.com.

37.11.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs.

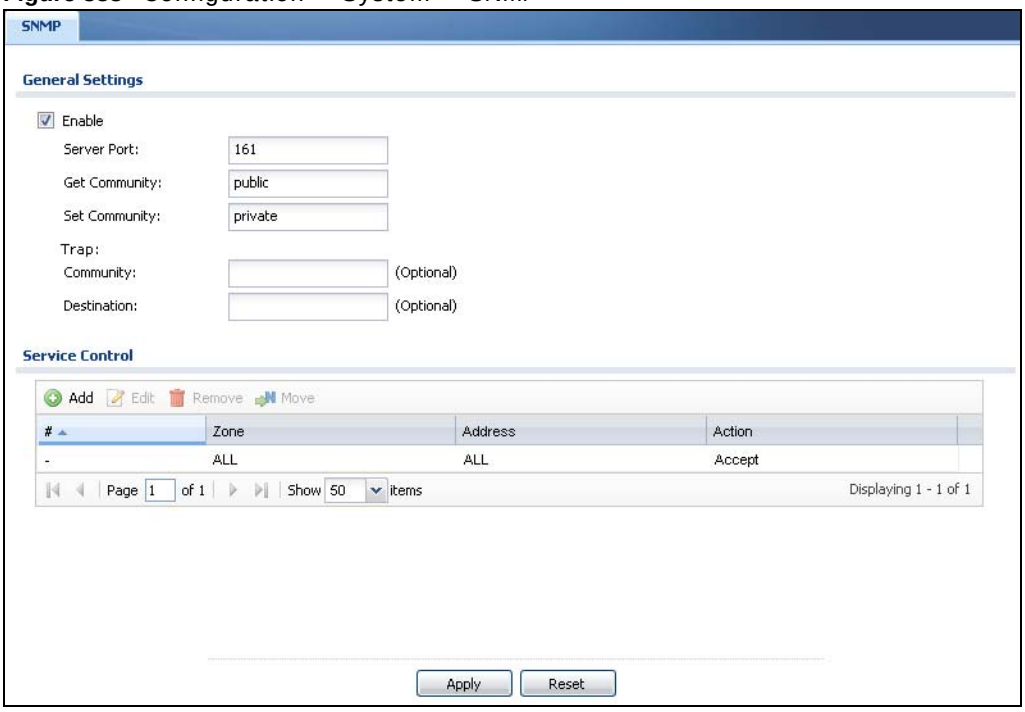
Table 190 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ZyWALL is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

37.11.3 Configuring SNMP

To change your ZyWALL's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

Figure 333 Configuration > System > SNMP



The following table describes the labels in this screen.

Table 191 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Service Control	This specifies from which computers you can access which ZyWALL zones.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. Refer to Table 185 on page 461 for details on the screen that opens.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The ZyWALL confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click **Move** to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.

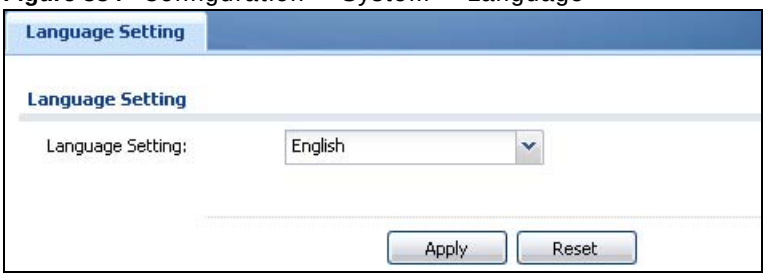
Table 191 Configuration > System > SNMP (continued)

LABEL	DESCRIPTION
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.12 Language Screen

Click **Configuration > System > Language** to open the following screen. Use this screen to select a display language for the ZyWALL's Web Configurator screens.

Figure 334 Configuration > System > Language



The following table describes the labels in this screen.

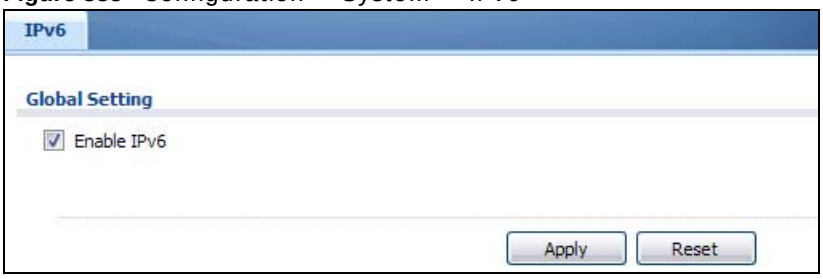
Table 192 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the ZyWALL's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

37.13 IPv6 Screen

Click **Configuration > System > IPv6** to open the following screen. Use this screen to enable IPv6 support for the ZyWALL's Web Configurator screens. See the IPv6 Overview on page 106 for more information about IPv6.

Figure 335 Configuration > System > IPv6



The following table describes the labels in this screen.

Table 193 Configuration > System > IPv6

LABEL	DESCRIPTION
Enable IPv6	Select this to have the ZyWALL support IPv6 and make IPv6 settings be available on the screens that the functions support, such as the **Configuration** > **Network** > **Interface** > **Ethernet**, **VLAN**, and **Bridge** screens. The ZyWALL discards all IPv6 packets if you clear this check box.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

38

Log and Report

38.1 Overview

Use these screens to configure daily reporting and log settings.

38.1.1 What You Can Do In this Chapter

- Use the **Email Daily Report** screen (Section 38.2 on page 485) to configure where and how to send daily reports and what reports to send.
- Use the **Log Setting** screens (Section 38.3 on page 487) to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers.

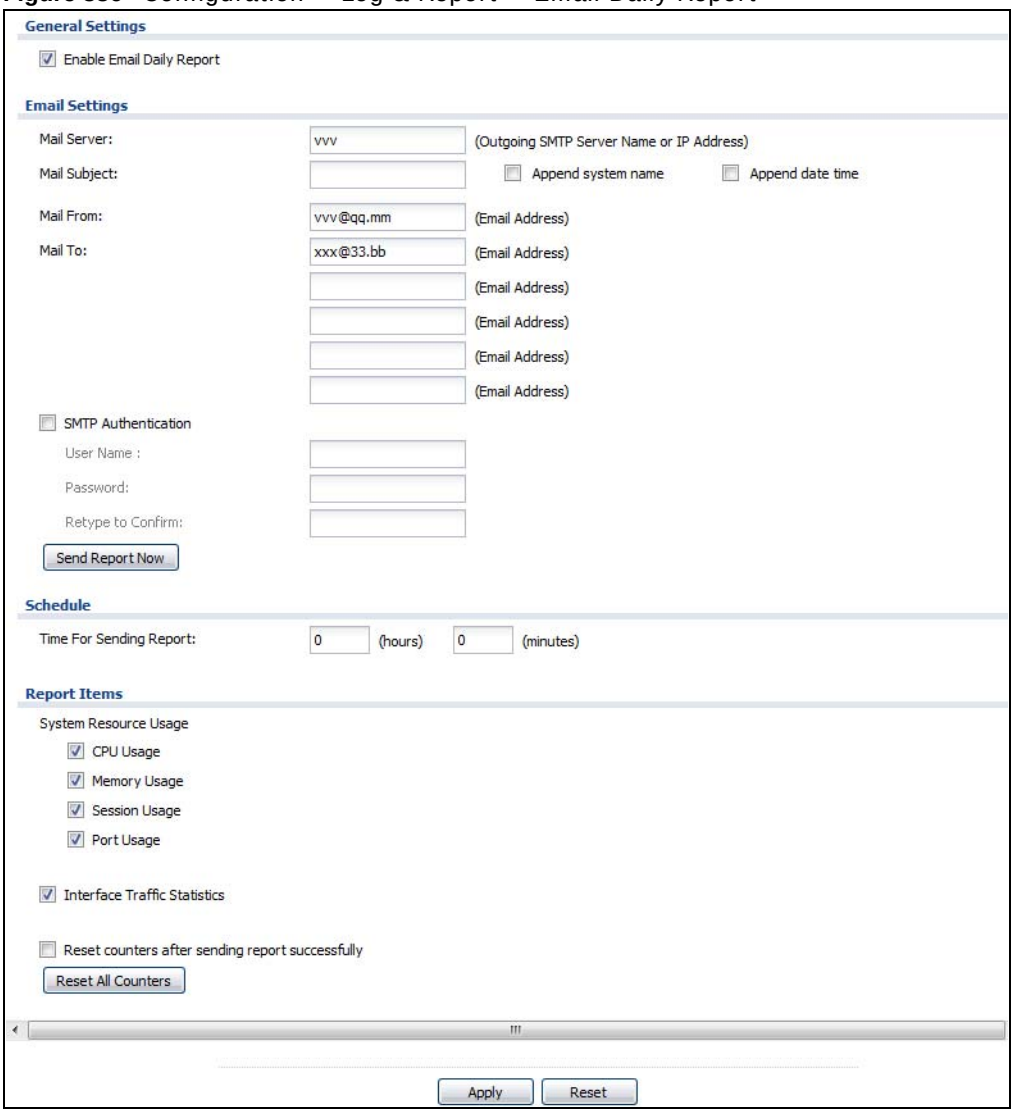
38.2 Email Daily Report

Use the **Email Daily Report** screen to start or stop data collection and view various statistics about traffic passing through your ZyWALL.

Note: Data collection may decrease the ZyWALL's traffic throughput rate.

Click **Configuration > Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the ZyWALL e-mail you system statistics every day.

Figure 336 Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 194 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the ZyWALL's system name to the subject. Select **Append date time** to add the ZyWALL's system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.

Table 194 Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Send Report Now	Click this button to have the ZyWALL send the daily e-mail report immediately.
Time for sending report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to return the screen to its last-saved settings.

38.3 Log Setting Screens

The **Log Setting** screens control log messages and alerts. A log message stores the information for viewing or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The ZyWALL provides a system log and supports e-mail profiles and remote syslog servers. View the system log in the **MONITOR > Log** screen. Use the e-mail profiles to mail log messages to the specific destinations. You can also have the ZyWALL store system logs on a connected USB storage device. The other four logs are stored on specified syslog servers.

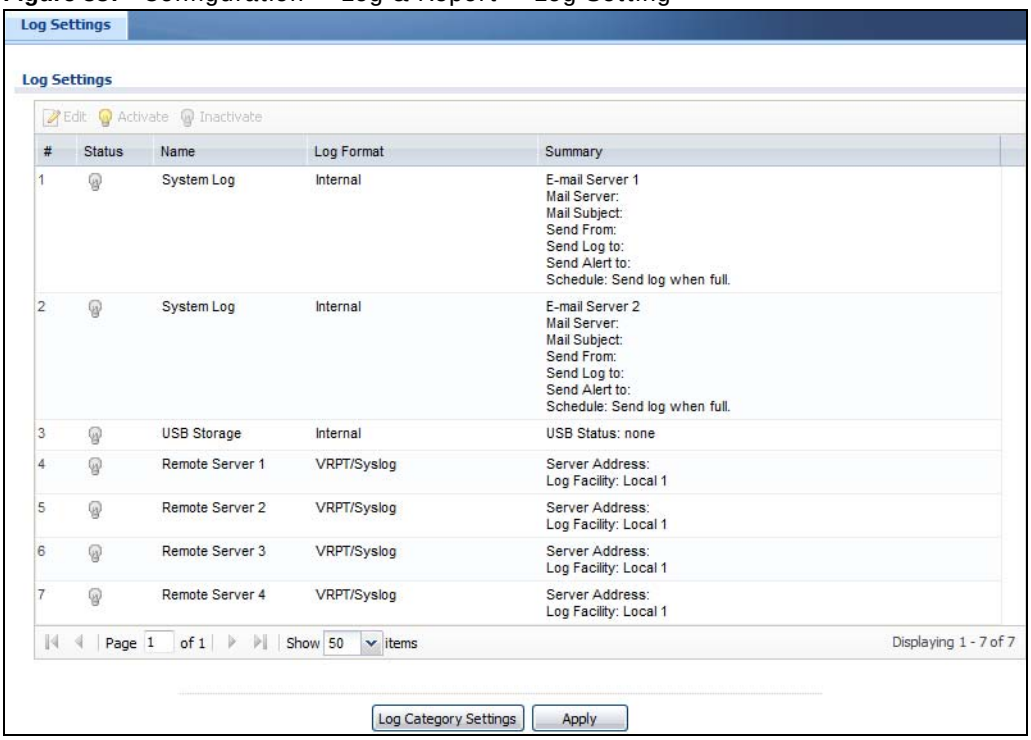
The **Log Setting** screens control what information the ZyWALL saves in each log. You can also specify which log messages to e-mail for the system log, and where and how often to e-mail them. These screens also set for which events to generate alerts and where to email the alerts.

The first **Log Setting** screen provides a settings summary. Use the **Edit** screens to configure settings such as log categories, e-mail addresses, and server names for any log. Use the **Log Category Settings** screen to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers.

38.3.1 Log Setting Summary

To access this screen, click **Configuration > Log & Report > Log Setting**.

Figure 337 Configuration > Log & Report > Log Setting


Log Settings
Log Settings
Edit
Activate
Inactivate
Status Name Log Format Summary
1 System Log Internal E-mail Server 1 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
2 System Log Internal E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3 USB Storage Internal USB Status: none
4 Remote Server 1 VRPT/Syslog Server Address: Log Facility: Local 1
5 Remote Server 2 VRPT/Syslog Server Address: Log Facility: Local 1
6 Remote Server 3 VRPT/Syslog Server Address: Log Facility: Local 1
7 Remote Server 4 VRPT/Syslog Server Address: Log Facility: Local 1
Page 1 of 1
Show 50 items
Displaying 1 - 7 of 7
Log Category Settings
Apply

The following table describes the labels in this screen.

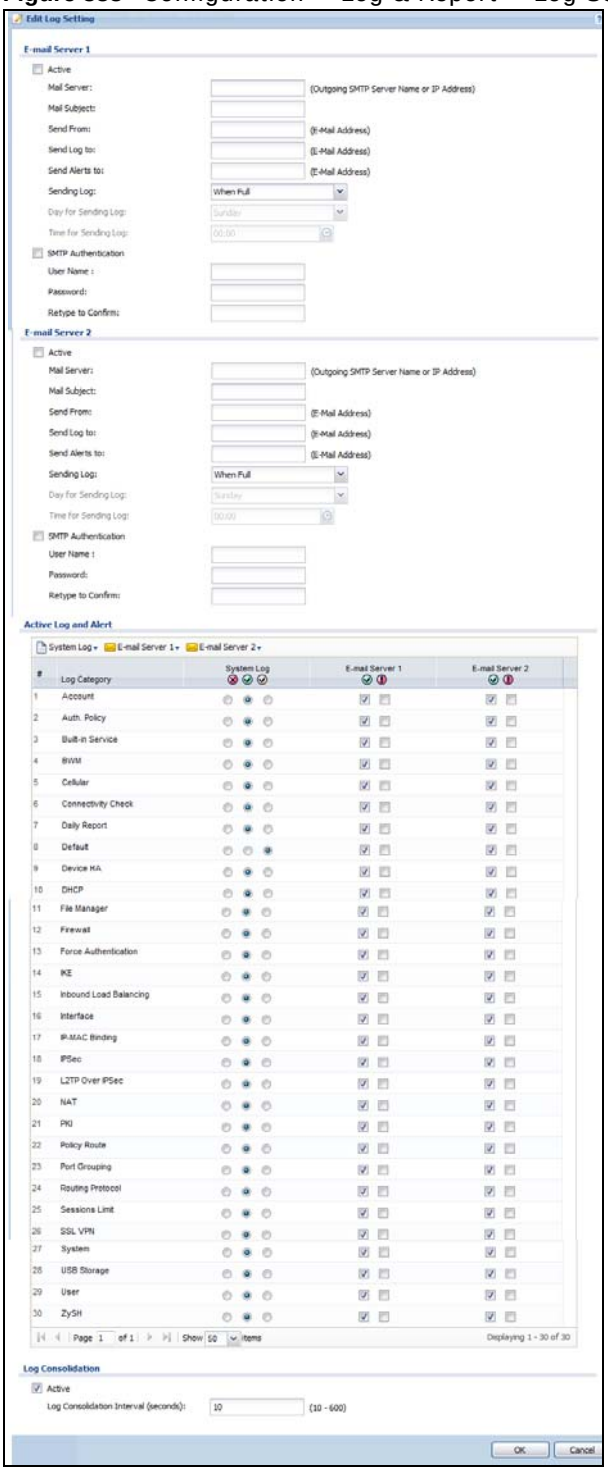
Table 195 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the ZyWALL, or one of the remote servers).
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 38.3.2 on page 489 for more information.
Log Category Settings	Click this button to open the **Log Category Settings Edit** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

38.3.2 Edit System Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings Summary** screen (see Section 38.3.1 on page 487), and click the system log **Edit** icon.

Figure 338 Configuration > Log & Report > Log Setting > Edit (System Log)



The following table describes the labels in this screen.

Table 196 Configuration > Log & Report > Log Setting > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Active Log and Alert	
System Log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the ZyWALL will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The ZyWALL does not e-mail debugging information, even if this setting is selected.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.

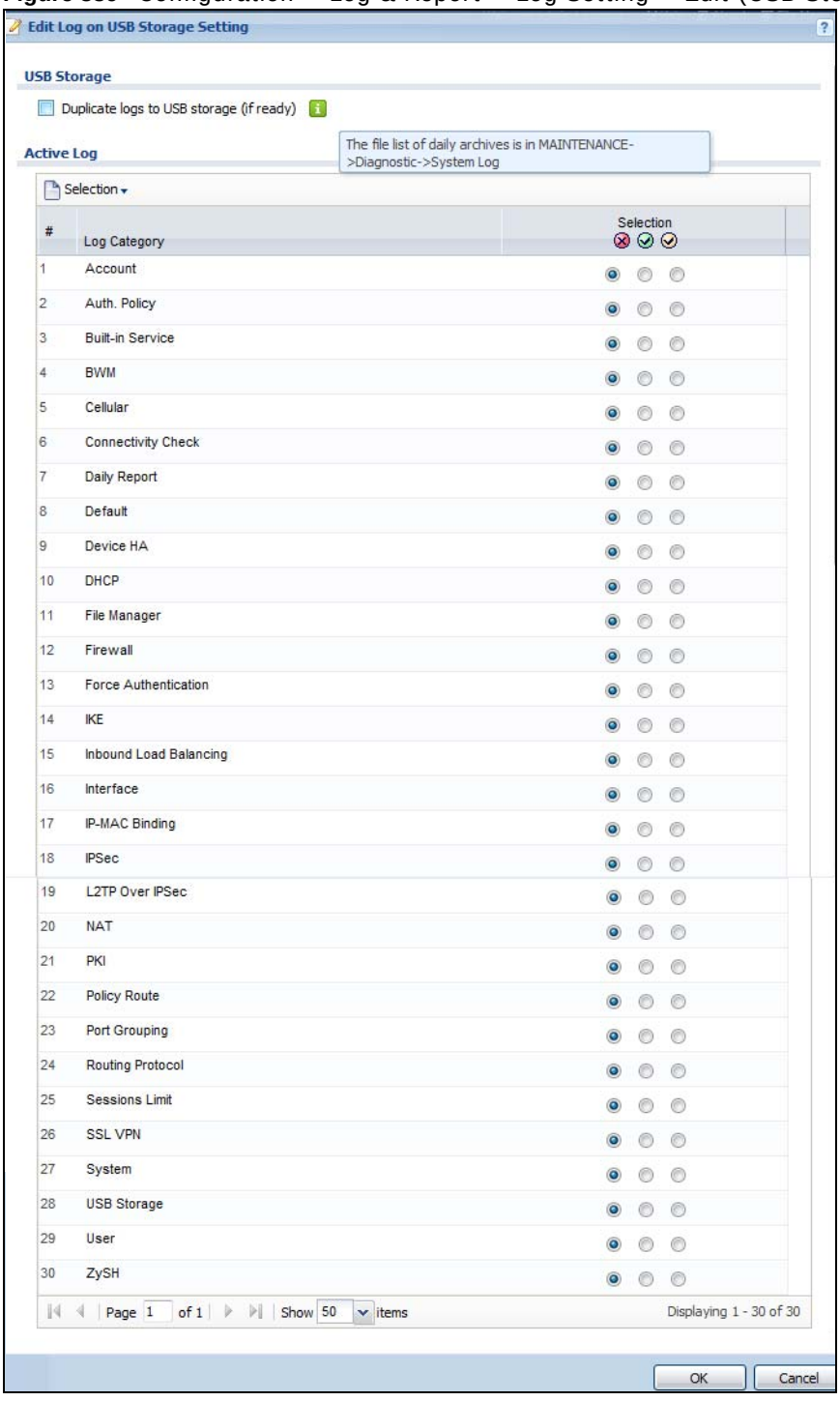
Table 196 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

LABEL	DESCRIPTION
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the ZyWALL does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

38.3.3 Edit Log on USB Storage Setting

The **Edit Log on USB Storage Setting** screen controls the detailed settings for saving logs to a connected USB storage device. Go to the **Log Setting Summary** screen (see Section 38.3.1 on page 487), and click the USB storage **Edit** icon.

Figure 339 Configuration > Log & Report > Log Setting > Edit (USB Storage)



The following table describes the labels in this screen.

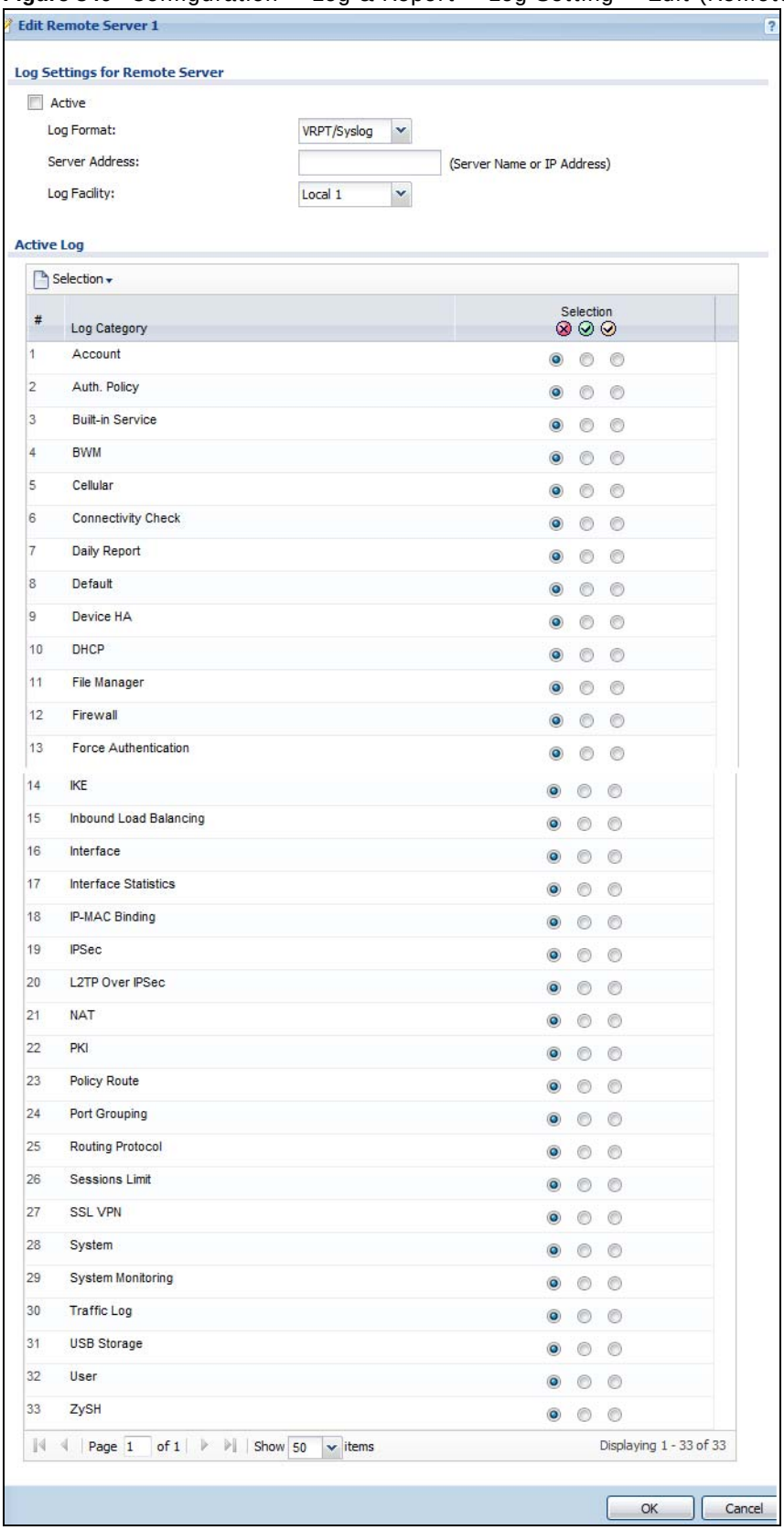
Table 197 Configuration > Log & Report > Log Setting > Edit (USB Storage)

LABEL	DESCRIPTION
Duplicate logs to USB storage (if ready)	Select this to have the ZyWALL save a copy of its system logs to a connected USB storage device. Use the **Active Log** section to specify what kinds of messages to include.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

38.3.4 Edit Remote Server Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see Section 38.3.1 on page 487), and click a remote server **Edit** icon.

Figure 340 Configuration > Log & Report > Log Setting > Edit (Remote Server)



The following table describes the labels in this screen.

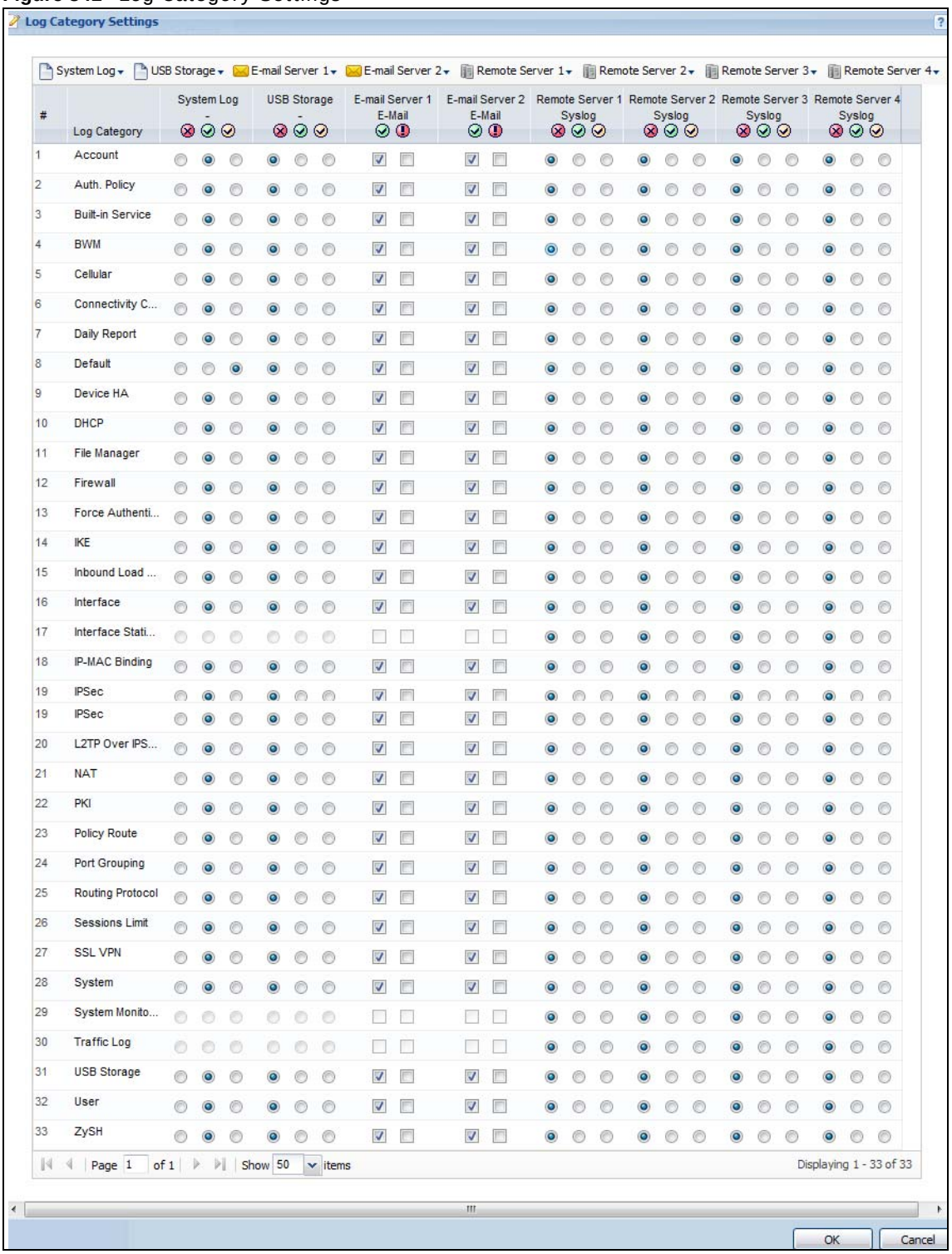
Table 198 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT / Syslog** - ZyXEL's Vantage Report, syslog-compatible format. **CEF / Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

38.3.5 Log Category Settings Screen

The **Log Category Settings** screen allows you to view and to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Settings Summary** screen (see Section 38.3.1 on page 487), and click the **Log Category Settings** button.

Figure 341 Log Category Settings



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 38.3.2 on page 489, where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 199 Configuration > Log & Report > Log Setting > Log Category Settings

LABEL	DESCRIPTION
System Log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the ZyWALL will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The ZyWALL does not e-mail debugging information, even if this setting is selected.
USB Storage	Use the **USB Storage** drop-down list to change the log settings for saving logs to a connected USB storage device. **disable all logs** (red X) - do not log any information for any category to a connected USB storage device. **enable normal logs** (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.

Table 199 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

LABEL	DESCRIPTION
System Log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the ZyWALL does not e-mail debugging information, however, even if this setting is selected.
USB Storage	Select which event log categories to save to a connected USB storage device. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - save log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - save log messages, alerts, and debugging information from this category.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**.
Remote Server 1~4	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

39

File Manager

39.1 Overview

Configuration files define the ZyWALL's settings. Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. You can apply a configuration file or run a shell script without the ZyWALL restarting. You can store multiple configuration files and shell script files on the ZyWALL. You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL. Configuration files use a .conf extension and shell scripts use a .zysh extension.

39.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see Section 39.2 on page 501) to store and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.
- Use the **Firmware Package** screen (see Section 39.3 on page 505) to check your current firmware version and upload firmware to the ZyWALL.
- Use the **Shell Script** screen (see Section 39.4 on page 507) to store, name, download, upload and run shell script files.

39.1.2 What you Need to Know

Configuration Files and Shell Scripts

When you apply a configuration file, the ZyWALL uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 342 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL applies configuration files differently than it runs shell scripts. This is explained below.

Table 200 Configuration Files and Shell Scripts in the ZyWALL

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Figure 342 on page 500 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the ZyWALL treat the line as a comment.

Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the ZyWALL exit sub command mode.

Note: "exit" or "!'" must follow sub commands if it is to make the ZyWALL exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface ge1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

39.2 The Configuration File Screen

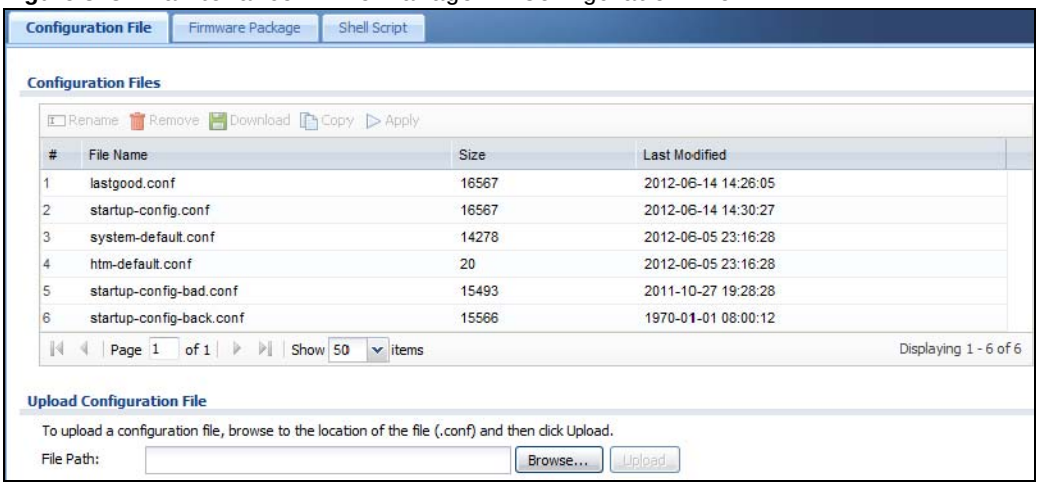
Click **Maintenance > File Manager > Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.

Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the ZyWALL (whether through a management interface or by physically turning the power off and back on), the ZyWALL uses the **system-default.conf** configuration file with the ZyWALL's default settings.
- If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the ZyWALL generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

Figure 343 Maintenance > File Manager > Configuration File



Do not turn off the ZyWALL while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 201 Maintenance > File Manager > Configuration File

LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the ZyWALL. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the ZyWALL. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen. **Figure 344** Maintenance > File Manager > Configuration File > Rename  Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the ZyWALL. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the ZyWALL. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen. **Figure 345** Maintenance > File Manager > Configuration File > Copy  Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 201 Maintenance > File Manager > Configuration File (continued)

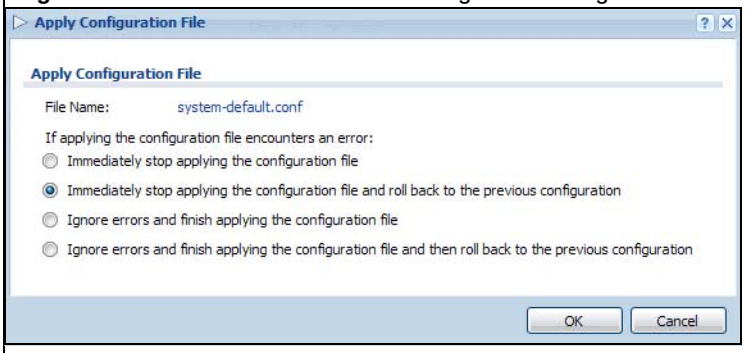
LABEL	DESCRIPTION
Apply	Use this button to have the ZyWALL use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the ZyWALL use that configuration file. The ZyWALL does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the ZyWALL is to do if it encounters an error in the configuration file. **Figure 346** Maintenance > File Manager > Configuration File > Apply  **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the ZyWALL started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the ZyWALL apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the ZyWALL with a fully valid configuration file. Click **OK** to have the ZyWALL start applying the configuration file or click **Cancel** to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.

Table 201 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the ZyWALL's default settings. Select this file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The ZyWALL applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your ZyWALL You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

39.3 The Firmware Package Screen

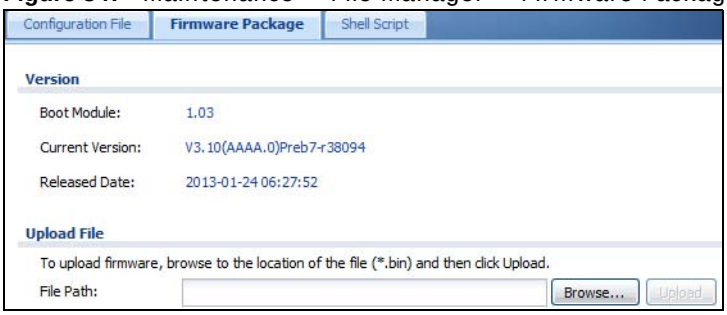
Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the ZyWALL.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin".

The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL while the firmware update is in progress!

Figure 347 Maintenance > File Manager > Firmware Package



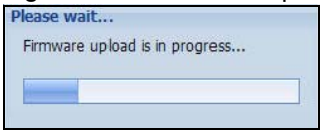
The following table describes the labels in this screen.

Table 202 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the ZyWALL.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

Figure 348 Firmware Upload In Process



Note: The ZyWALL automatically reboots after a successful upload.

The ZyWALL automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 349 Network



After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 350 Firmware Upload Error



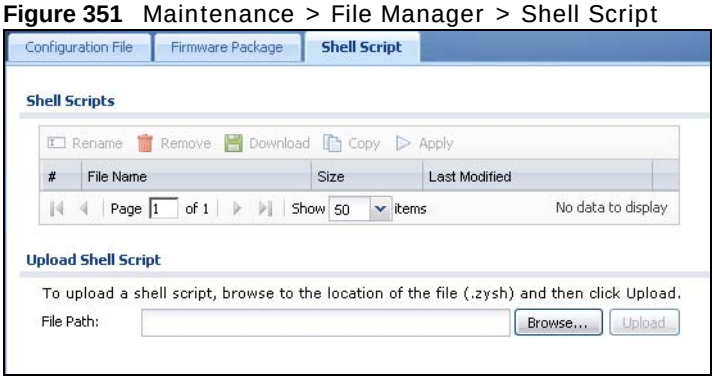
39.4 The Shell Script Screen

Use shell script files to have the ZyWALL use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the ZyWALL at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the ZyWALL restarts. You could use multiple `write` commands in a long script.

Figure 351 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 203 Maintenance > File Manager > Shell Script

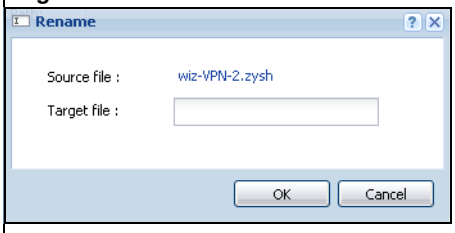
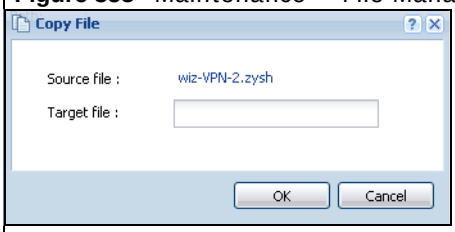
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the ZyWALL. You cannot rename a shell script to the name of another shell script in the ZyWALL. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. **Figure 352** Maintenance > File Manager > Shell Script > Rename  Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Remove** to delete the shell script file from the ZyWALL. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the ZyWALL. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. **Figure 353** Maintenance > File Manager > Shell Script > Copy  Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the ZyWALL use a specific shell script file. Click a shell script file's row to select it and click **Apply** to have the ZyWALL use that shell script file. You may need to wait awhile for the ZyWALL to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.

Table 203 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ZyWALL.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

40

Diagnostics

40.1 Overview

Use the diagnostics screens for troubleshooting.

40.1.1 What You Can Do in this Chapter

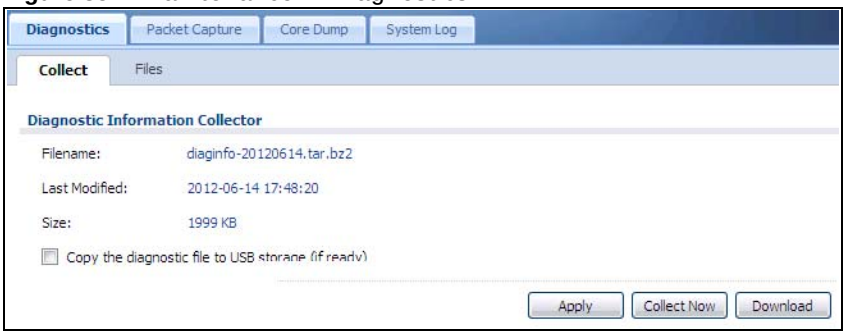
- Use the **Diagnostics** screen (see Section 40.2 on page 510) to generate a file containing the ZyWALL's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the **Packet Capture** screens (see Section 40.3 on page 512) to capture packets going through the ZyWALL.
- Use the **Core Dump** screens (see Section 40.4 on page 515) to have the ZyWALL save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes) so you can send the file to customer support for troubleshooting.
- Use the **System Log** screens (see Section 40.5 on page 516) to download files of system logs from a connected USB storage device to your computer.

40.2 The Diagnostic Screen

The **Diagnostic** screen provides an easy way for you to generate a file containing the ZyWALL's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

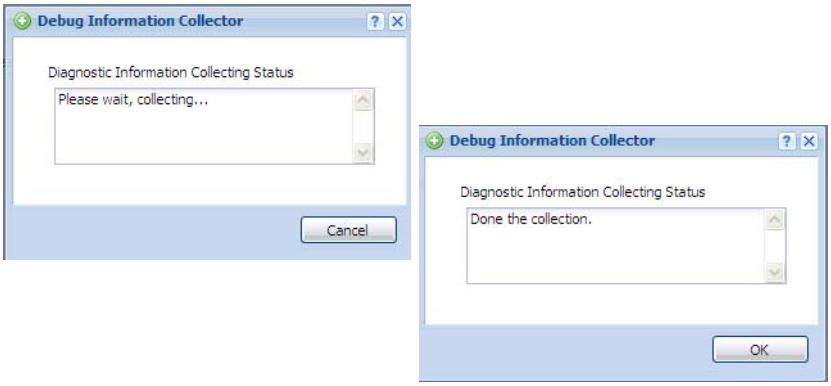
Click **Maintenance > Diagnostics** to open the **Diagnostic** screen.

Figure 354 Maintenance > Diagnostics



The following table describes the labels in this screen.

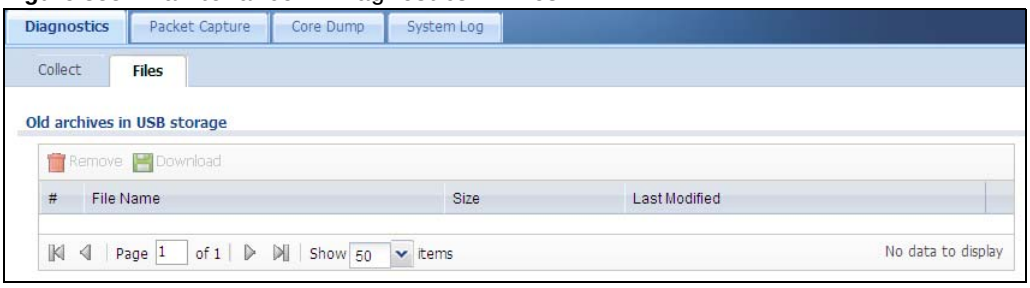
Table 204 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Copy the diagnostic file to USB storage (if ready)	Select this to have the ZyWALL create an extra copy of the diagnostic file to a connected USB storage device.
Apply	Click **Apply** to save your changes.
Collect Now	Click this to have the ZyWALL create a new diagnostic file. Wait while information is collected. 
Download	Click this to save the most recent diagnostic file to a computer.

40.2.1 The Diagnostics Files Screen

Click **Maintenance > Diagnostics > Files** to open the diagnostic files screen. This screen lists the files of diagnostic information the ZyWALL has collected and stored in a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 355 Maintenance > Diagnostics > Files



The following table describes the labels in this screen.

Table 205 Maintenance > Diagnostics > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ZyWALL. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.

Table 205 Maintenance > Diagnostics > Files (continued)

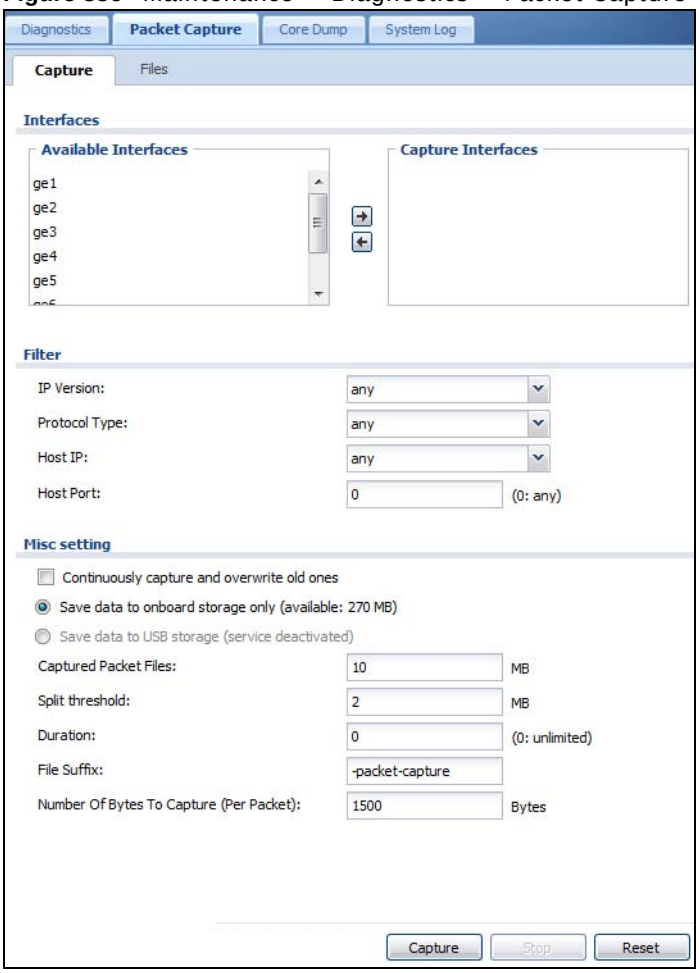
LABEL	DESCRIPTION
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

40.3 The Packet Capture Screen

Use this screen to capture network traffic going through the ZyWALL's interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostics > Packet Capture** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the **File Suffix** field's setting to avoid this.

Figure 356 Maintenance > Diagnostics > Packet Capture



The following table describes the labels in this screen.

Table 206 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under **Available Interfaces**. Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
IP Version	Select the version of IP for which to capture packets. Select **any** to capture packets for all IP versions.
Protocol Type	Select the protocol of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.
Host Port	This field is configurable when you set the **IP Type** to **any**, **tcp**, or **udp**. Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the ZyWALL keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.
Save data to onboard storage only	Select this to have the ZyWALL only store packet capture entries on the ZyWALL. The available storage size is displayed as well. Note: The ZyWALLL reserves some onboard storage space as a buffer.
Save data to USB storage	Select this to have the ZyWALL store packet capture entries only on a USB storage device connected to the ZyWALL if the ZyWALL allows this. Status: **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the ZyWALL cannot mount it. **none** - no USB storage device is connected. **service deactivated** - USB storage feature is disabled (in **Configuration > Object > USB Storag**e), so the ZyWALL cannot use a connected USB device to store system logs and other diagnostic information. **available** - you can have the ZyWALL use the USB storage device. The available storage capacity also displays. Note: The ZyWALL reserves some USB storage space as a buffer.
Captured Packet Files	When saving packet captures only to the ZyWALL's onboard storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the ZyWALL. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the **Continuously capture and overwrite old ones** option, you may need to set this size larger or delete existing capture files. The valid range depends on the available onboard/USB storage size. The ZyWALL stops the capture and generates the capture file when either the file reaches this size or the time period specified in the **Duration** field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the ZyWALL starts another packet capture file.

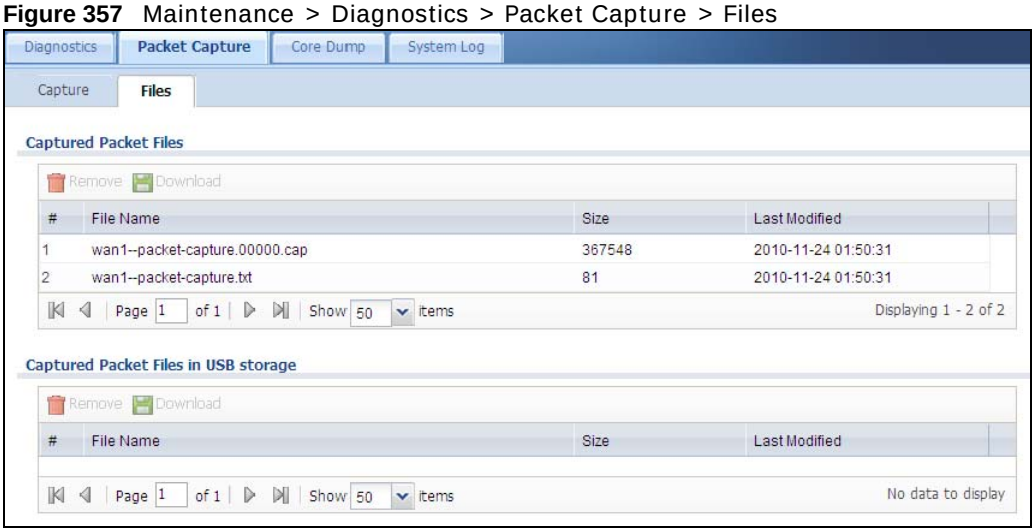
Table 206 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Duration	Set a time limit in seconds for the capture. The ZyWALL stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the **File Size** field. 0 means there is no time limit.
File Suffix	Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is “interface name-file suffix.cap”, for example “vlan2-packet-capture.cap”.
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The ZyWALL automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
Capture	Click this button to have the ZyWALL capture packets according to the settings configured in this screen. You can configure the ZyWALL while a packet capture is in progress although you cannot modify the packet capture settings. The ZyWALL’s throughput or performance may be affected while a packet capture is in progress. After the ZyWALL finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

40.3.1 The Packet Capture Files Screen

Click **Maintenance > Diagnostics > Packet Capture > Files** to open the packet capture files screen. This screen lists the files of packet captures stored on the ZyWALL or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 357 Maintenance > Diagnostics > Packet Capture > Files



The following table describes the labels in this screen.

Table 207 Maintenance > Diagnostics > Packet Capture > Files

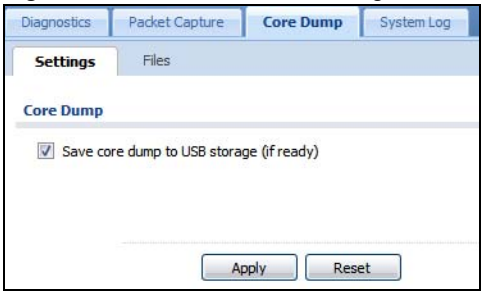
LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ZyWALL or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

40.4 Core Dump Screen

Use the **Core Dump** screen to have the ZyWALL save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics > Core Dump** to open the following screen.

Figure 358 Maintenance > Diagnostics > Core Dump



The following table describes the labels in this screen.

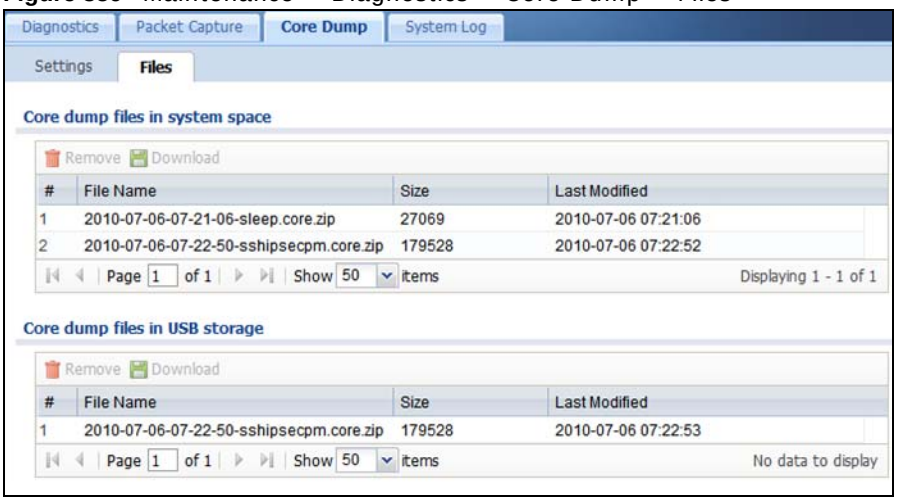
Table 208 Maintenance > Diagnostics > Core Dump

LABEL	DESCRIPTION
Save core dump to USB storage (if ready)	Select this to have the ZyWALL save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). If you clear this option the ZyWALL only saves
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

40.4.1 Core Dump Files Screen

Click **Maintenance > Diagnostics > Core Dump > Files** to open the core dump files screen. This screen lists the core dump files stored on the ZyWALL or a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 359 Maintenance > Diagnostics > Core Dump > Files


Diagnostics
Packet Capture
Core Dump
System Log
Settings
Files
Core dump files in system space
Remove
Download
File Name Size Last Modified
1 2010-07-06-07-21-06-sleep.core.zip 27069 2010-07-06 07:21:06
2 2010-07-06-07-22-50-sshipsecpm.core.zip 179528 2010-07-06 07:22:52
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1
Core dump files in USB storage
Remove
Download
File Name Size Last Modified
1 2010-07-06-07-22-50-sshipsecpm.core.zip 179528 2010-07-06 07:22:53
Page 1 of 1 Show 50 items No data to display

The following table describes the labels in this screen.

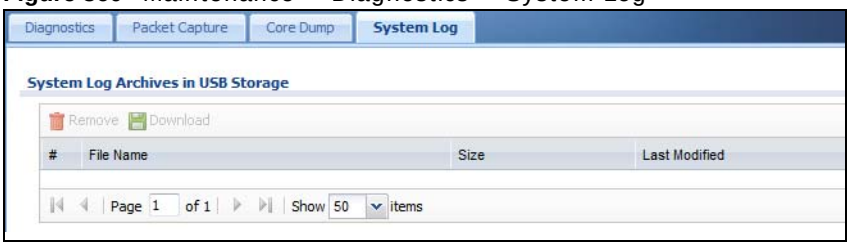
Table 209 Maintenance > Diagnostics > Core Dump > Files

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ZyWALL. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

40.5 The System Log Screen

Click **Maintenance > Diagnostics > System Log** to open the system log files screen. This screen lists the files of system logs stored on a connected USB storage device. The files are in comma separated value (csv) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 360 Maintenance > Diagnostics > System Log



The following table describes the labels in this screen.

Table 210 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Remove	Select files and click **Remove** to delete them from the ZyWALL. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click **Download** to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

41

Packet Flow Explore

41.1 Overview

Use this to get a clear picture on how the ZyWALL determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

41.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see Section 41.2 on page 518) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see Section 41.3 on page 522) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

41.2 The Routing Status Screen

The **Routing Status** screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the **Routing Flow** section, the related routes (activated) will display in the **Routing Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore**.

The order of the routing flow may vary depending on whether you:

- select **use policy route to override direct route** in the **CONFIGURATION > Network > Routing > Policy Route** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- select **use policy routes to control dynamic IPSec rules** in the **CONFIGURATION > VPN > IPSec VPN > VPN Connection** screen.

Note: Once a packet matches the criteria of a routing rule, the ZyWALL takes the corresponding action and does not perform any further flow checking.

Figure 361 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

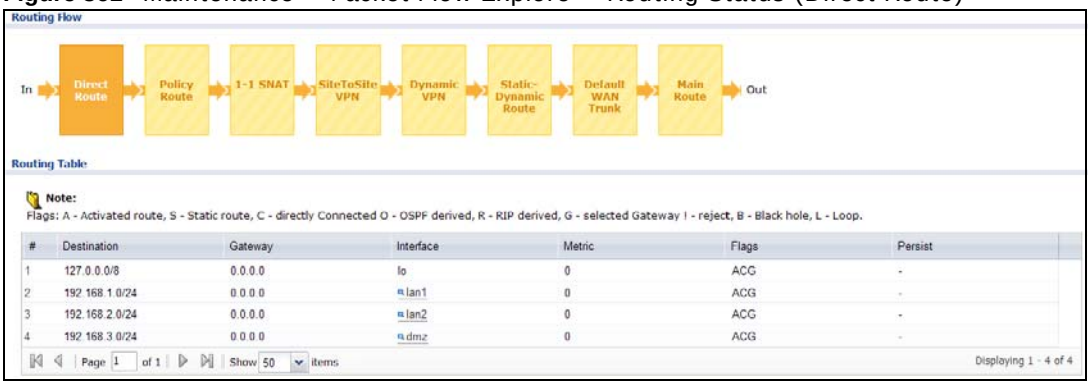

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Main Route
Out
Routing Table
Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.
Destination Gateway Interface Metric Flags Persist
1 127.0.0.0/8 0.0.0.0 lo 0 ACG -
2 192.168.1.0/24 0.0.0.0 lan1 0 ACG -
3 192.168.2.0/24 0.0.0.0 lan2 0 ACG -
4 192.168.3.0/24 0.0.0.0 dmz 0 ACG -
Page 1 of 1 Show 50 items
Displaying 1 - 4 of 4

Figure 362 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

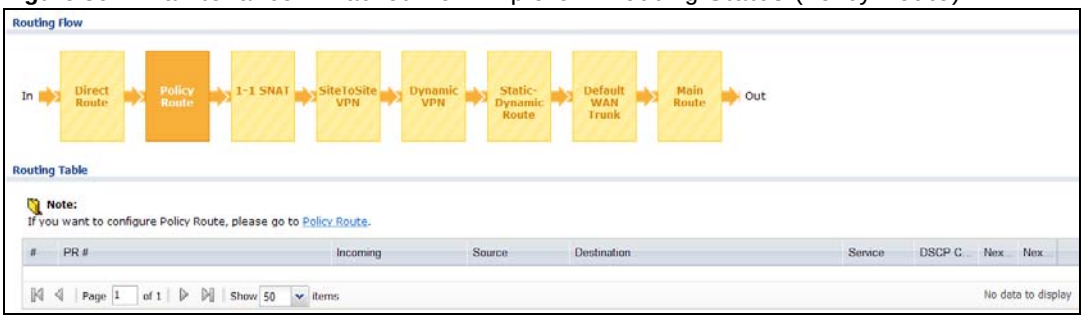


Figure 363 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

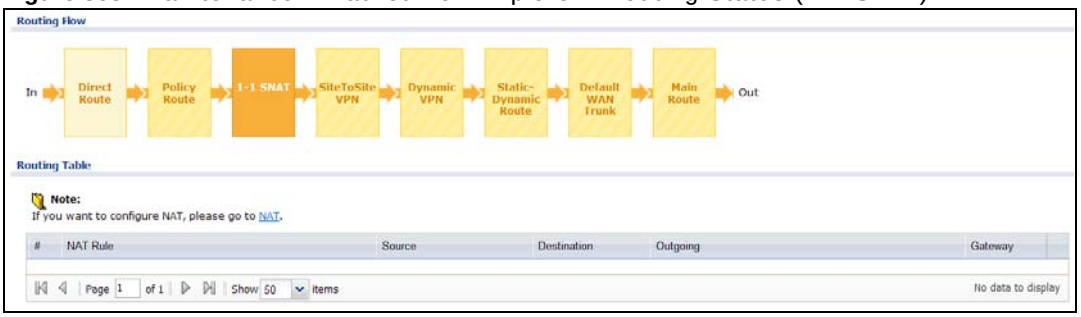


Figure 364 Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)

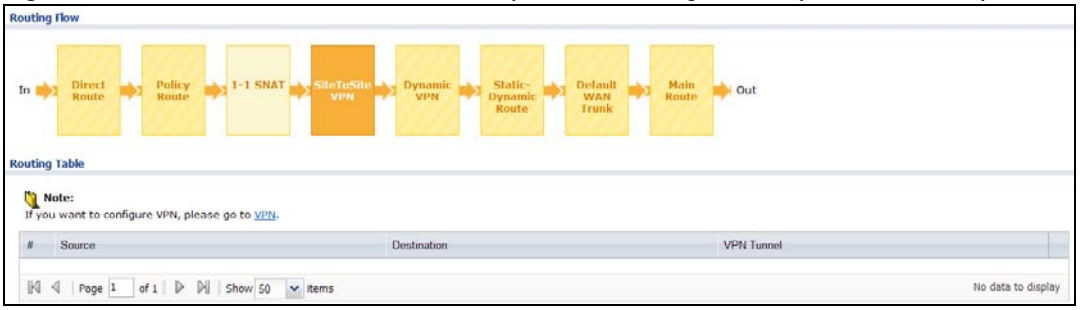


Figure 365 Maintenance > Packet Flow Explore > Routing Status (Dynamic VPN)

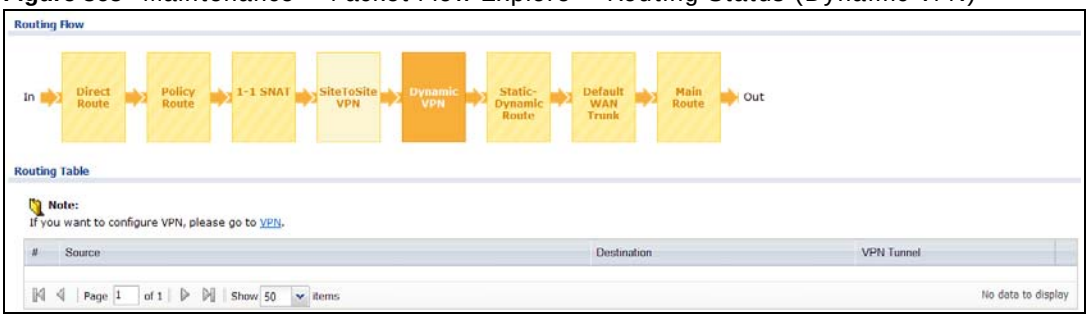


Figure 366 Maintenance > Packet Flow Explore > Routing Status (Static-Dynamic Route)

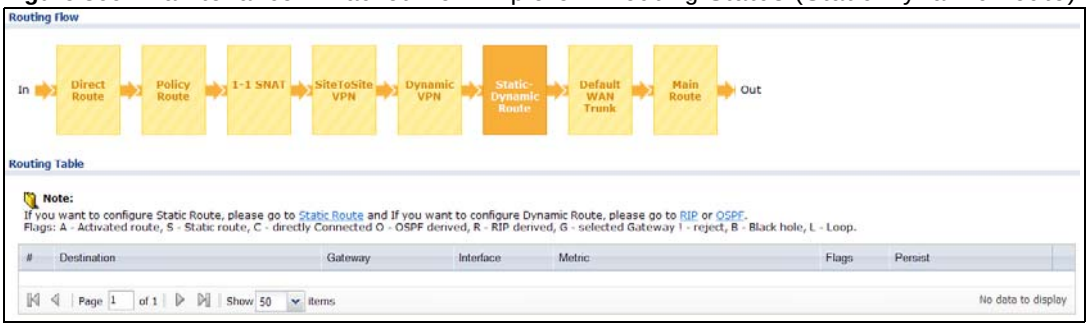

Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Main Route
Out
Routing Table
Note:
If you want to configure Static Route, please go to Static Route and If you want to configure Dynamic Route, please go to RIP or OSPF.
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.
Destination Gateway Interface Metric Flags Persist
Page 1 of 1 Show 50 items
No data to display

Figure 367 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

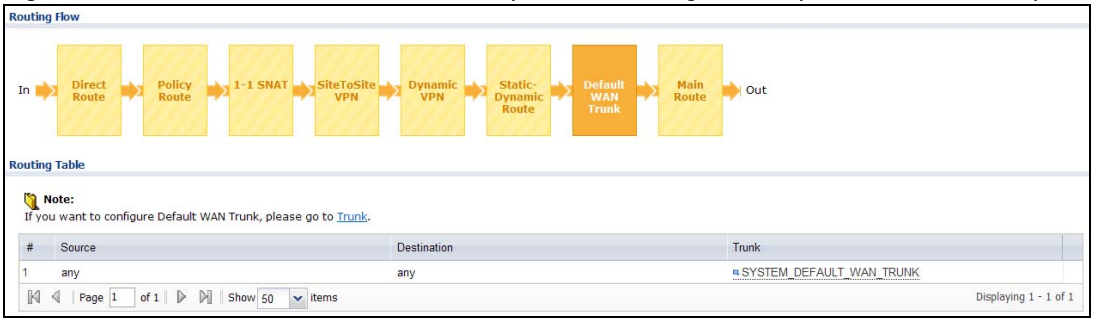
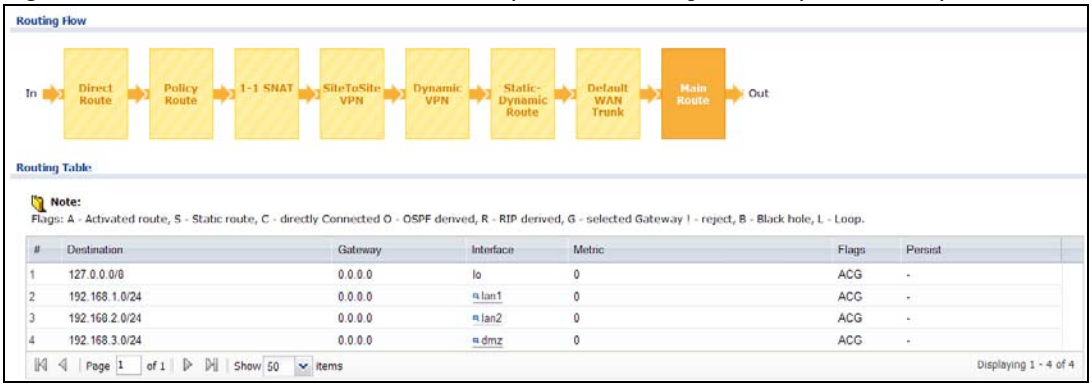


Figure 368 Maintenance > Packet Flow Explore > Routing Status (Main Route)


Routing Flow
In
Direct Route
Policy Route
1-1 SNAT
SiteToSite VPN
Dynamic VPN
Static-Dynamic Route
Default WAN Trunk
Main Route
Out
Routing Table
Note:
Flags: A - Activated route, S - Static route, C - directly Connected O - OSPF derived, R - RIP derived, G - selected Gateway ! - reject, B - Black hole, L - Loop.
Destination Gateway Interface Metric Flags Persist
1 127.0.0.0/8 0.0.0.0 lo 0 ACG -
2 192.168.1.0/24 0.0.0.0 lan1 0 ACG -
3 192.168.2.0/24 0.0.0.0 lan2 0 ACG -
4 192.168.3.0/24 0.0.0.0 dmz 0 ACG -
Page 1 of 1 Show 50 items
Displaying 1 - 4 of 4

The following table describes the labels in this screen.

Table 211 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the ZyWALL determines where to route a packet. Click a function box to display the related settings in the **Routing Table** section.
Routing Table	This section shows the corresponding settings according to the function box you click in the **Routing Flow** section.
The following fields are available if you click **Direct Route**, **Static-Dynamic Route**, or **Main Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: • **A** - this route is currently activated • **S** - this is a static route • **C** - this is a direct connected route • **O** - this is a dynamic route learned through OSPF • **R** - this is a dynamic route learned through RIP • **G** - the route is to a gateway (router) in the same network. • **!** - this is a route which forces a route lookup to fail. • **B** - this is a route which discards packets. • **L** - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The ZyWALL removes the route after this time period is counted down to zero.
The following fields are available if you click **Policy Route** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route. If you have configured a schedule for the route, this screen only displays the route at the scheduled time.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. **any** means all services.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 9.2 on page 189 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	• This is the main route if the next hop type is **Auto**. • This is the interface name and gateway IP address if the next hop type is **Interface / GW**. • This is the tunnel name if the next hop type is **VPN Tunnel**. • This is the trunk name if the next hop type is **Trunk**.
The following fields are available if you click **1-1 SNAT** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.

Table 211 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Outgoing	This is the name of an interface which transmits packets out of the ZyWALL.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click **SiteToSite VPN** or **Dynamic VPN** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click **Default WAN Trunk** in the **Routing Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. **any** means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. **any** means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

41.3 The SNAT Status Screen

The **SNAT Status** screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the **SNAT Flow** section, the related SNAT rules (activated) will display in the **SNAT Table** section. To access this screen, click **Maintenance** > **Packet Flow Explore** > **SNAT Status**.

The order of the SNAT flow may vary depending on whether you:

- select **use default SNAT** in the **CONFIGURATION > Network > Interface > Trunk** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the ZyWALL takes the corresponding action and does not perform any further flow checking.

Figure 369 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

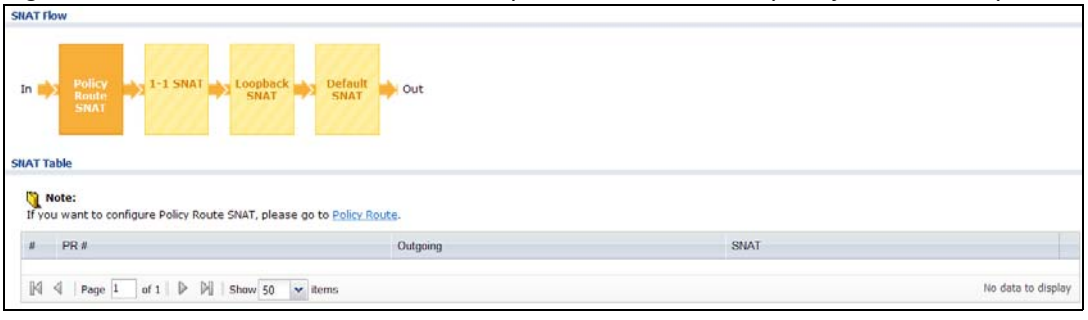


Figure 370 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

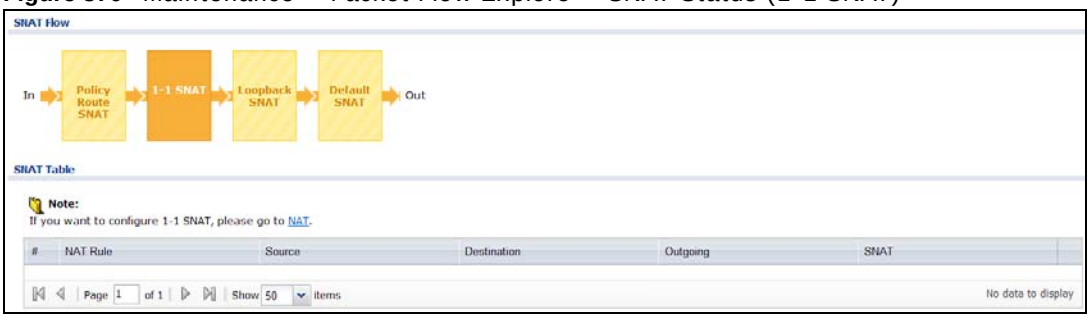


Figure 371 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

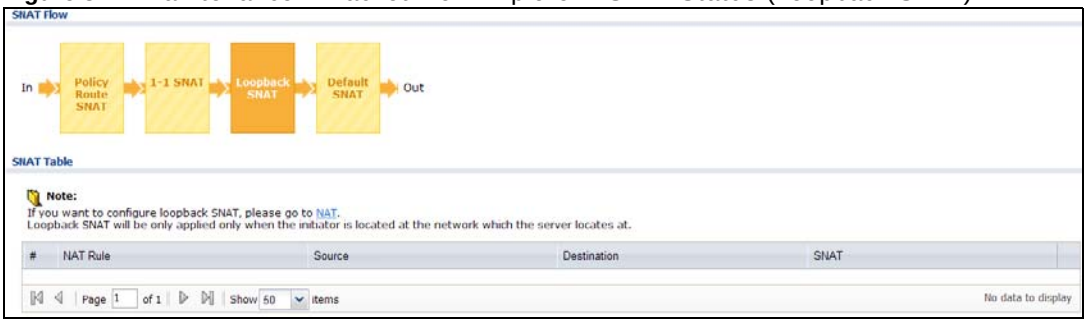
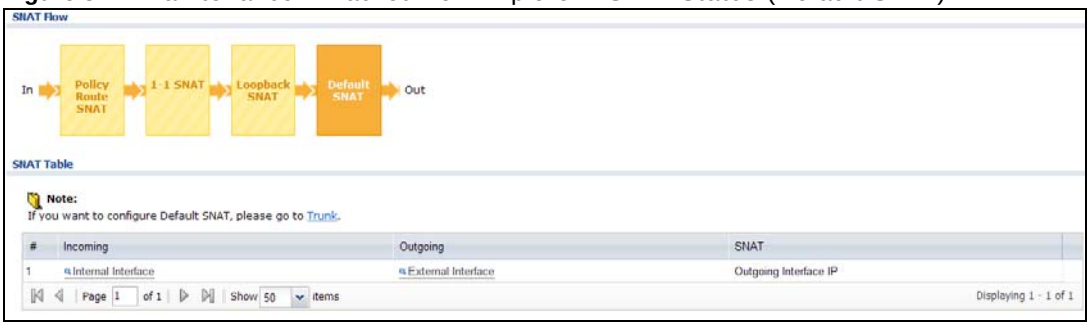

SNAT Flow
In
Policy Route SNAT
1-1 SNAT
Loopback SNAT
Default SNAT
Out
SNAT Table
Note:
If you want to configure loopback SNAT, please go to NAT.
Loopback SNAT will be only applied only when the initiator is located at the network which the server locates at.
NAT Rule Source Destination SNAT
Page 1 of 1 Show 50 items
No data to display

Figure 372 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

Table 212 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the ZyWALL changes the source IP address for a packet according to the rules you have configured in the ZyWALL. Click a function box to display the related settings in the **SNAT Table** section.
SNAT Table	The table fields in this section vary depending on the function box you select in the **SNAT Flow** section.
The following fields are available if you click **Policy Route SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route which uses SNAT.
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **1-1 SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the original source IP address(es).

Table 212 Maintenance > Packet Flow Explore > SNAT Status (continued)

LABEL	DESCRIPTION
Destination	This is the original destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click **Loopback SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the ZyWALL uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click **Default SNAT** in the **SNAT Flow** section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, **Outgoing Interface IP** means that the ZyWALL uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

42

Reboot

42.1 Overview

Use this to restart the device (for example, if the device begins behaving erratically). See also Section on page 31 for information on different ways to start and stop the ZyWALL.

42.1.1 What You Need To Know

If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see Section 44.1 on page 535) reset returns the device to its default configuration.

42.2 The Reboot Screen

The **Reboot** screen allows remote users to restart the device. To access this screen, click **Maintenance** > **Reboot**.

Figure 373 Maintenance > Reboot


Reboot
Reboot
Click the Reboot button to reboot the device. Please wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.
Reboot

Click the **Reboot** button to restart the ZyWALL. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the ZyWALL.

43

Shutdown

43.1 Overview

Use this to shutdown the device in preparation for disconnecting the power. See also Section on page 31 for information on different ways to start and stop the ZyWALL.

Always use the Maintenance > Shutdown > Shutdown screen or the "shutdown" command before you turn off the ZyWALL or remove the power. Not doing so can cause the firmware to become corrupt.

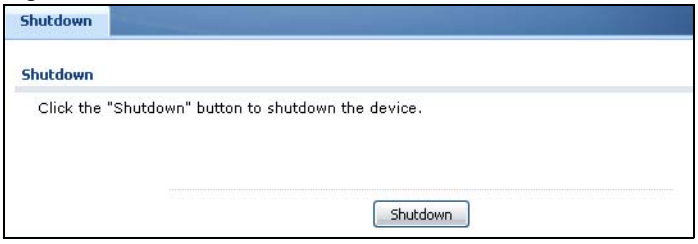
43.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

43.2 The Shutdown Screen

To access this screen, click **Maintenance** > **Shutdown**.

Figure 374 Maintenance > Shutdown



Click the **Shutdown** button to shut down the ZyWALL. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command shutdown to shutdown the ZyWALL.

44

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Chapter 6 on page 100).
- For the order in which the ZyWALL applies its features and checks, see Chapter 41 on page 518.

None of the LEDs turn on.

Make sure that you have the power cord connected to the ZyWALL and plugged in to an appropriate power source. Make sure you have the ZyWALL turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Cannot access the ZyWALL from the LAN.

- Check the cable connection between the ZyWALL and your computer or switch.
- Ping the ZyWALL from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the ZyWALL's.
- In the computer, click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the ZyWALL's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The ZyWALL should reply.
- If you've forgotten the ZyWALL's password, use the **RESET** button. Press the button in for about 5 seconds (or until the **PWR** LED starts to blink), then release it. It returns the ZyWALL to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your User's Guide for details).

I cannot access the Internet.

- Check the ZyWALL's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- Check the WAN interface's status in the **Dashboard**. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

I configured security settings but the ZyWALL is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The ZyWALL is not applying the custom policy route I configured.

The ZyWALL checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that the traffic would also match.

The ZyWALL is not applying the custom firewall rule I configured.

The ZyWALL checks the firewall rules in the order that they are listed. So make sure that your custom firewall rule comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

The format of interface names other than the Ethernet interface names is very strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

My rules and settings that apply to a particular interface no longer work.

The interface's IP address may have changed. To avoid this create an IP address object based on the interface. This way the ZyWALL automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

You have to set up an ISP account before you create a PPPoE or PPTP interface.

The data rates through my cellular connection are no-where near the rates I expected.

The actual cellular data rate you obtain varies depending on the cellular device you use, the signal strength to the service provider's base station, and so on.

I created a cellular interface but cannot connect through it.

- Make sure you have a compatible 3G device installed or connected. See www.zyxel.com for details.
- Make sure you have the cellular interface enabled.
- Make sure the cellular interface has the correct user name, password, and PIN code configured with the correct casing.
- If the ZyWALL has multiple WAN interfaces, make sure their IP addresses are on different subnets.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

Each VLAN interface is created on top of only one Ethernet interface.

The ZyWALL is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the ZyWALL does not support ingress bandwidth management.

The ZyWALL is not scanning some zipped files.

The ZyWALL cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the ZyWALL can concurrently unzip.

The ZyWALL is deleting some zipped files.

The ZyWALL cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the ZyWALL can concurrently unzip.

The ZyWALL routes and applies SNAT for traffic from some interfaces but not from others.

The ZyWALL automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **General**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the **Interface Type** set to **Internal** or **External**.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.
- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the ZyWALL.
- You may need to configure the DDNS entry's IP Address setting to **Auto** if the interface has a dynamic IP address or there are one or more NAT routers between the ZyWALL and the DDNS server.
- The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

The ZyWALL keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can set the ZyWALL's firewall to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate

subnets. See Asymmetrical Routes on page 268 and the chapter about interfaces for more information.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both ZyXEL IPSec routers and check the settings in each field methodically and slowly. Make sure both the ZyWALL and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 20 on page 281.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- The ZyWALL and remote IPSec router must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode.
- Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.
- When using manual keys, the ZyWALL and remote IPSec router must use the same encryption key and authentication key.
- When using pre-shared keys, the ZyWALL and the remote IPSec router must use the same pre-shared key.
- The ZyWALL's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- The ZyWALL and remote IPSec router must use the same active protocol.
- The ZyWALL and remote IPSec router must use the same encapsulation.
- The ZyWALL and remote IPSec router must use the same SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the ZyWALL and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following ZyWALL features.

- The ZyWALL does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Chapter 9 on page 187.
- Make sure the To-ZyWALL firewall rules allow IPSec VPN traffic to the ZyWALL. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The ZyWALL supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-ZyWALL firewall rules allow UDP port 4500 too.

- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the ZyWALL sends before the ZyWALL encrypts them and check packets the ZyWALL receives after the ZyWALL decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the ZyWALL and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the ZyWALL and remote IPSec router first and make sure they trust each other's certificates. If the ZyWALL's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The ZyWALL uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

If you have the **Configuration > VPN > IPSec VPN > VPN Connection** screen's **Use Policy Route to control dynamic IPSec rules option** enabled, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

I uploaded a logo to show in the SSL VPN user screens but it does not display properly.

The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

I logged into the SSL VPN but cannot see some of the resource links.

Available resource links vary depending on the SSL application object's configuration.

I changed the LAN IP address and can no longer access the Internet.

The ZyWALL automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I cannot get the RADIUS server to authenticate the ZyWALL's default admin account.

The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 31 on page 400 for more information about authentication methods.)

The ZyWALL fails to authentication the ext-user user accounts I configured.

An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts. If the ZyWALL tries to use the local database to authenticate an **ext-user**, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in Chapter 31 on page 400 and Chapter 32 on page 409, respectively.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default **admin** account into any user group.

The schedule I configured is not being applied at the configured times.

Make sure the ZyWALL's current date and time are correct.

I cannot get a certificate to import into the ZyWALL.

1. For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the ZyWALL. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.
2. You must remove any spaces from the certificate's filename before you can import the certificate.
3. Any certificate that you want to import has to be in one of these file formats:
   - Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
   - PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
   - Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.

- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I cannot access the ZyWALL from a computer connected to the Internet.

Check the service control rules and to-ZyWALL firewall rules.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The ZyWALL's traffic throughput rate decreased after I started collecting traffic statistics.

Data collection may decrease the ZyWALL's traffic throughput rate.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the ZyWALL treat the line as a comment.

- Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the ZyWALL restarts. You could use multiple `write` commands in a long script.

Note: “exit” or “!'” must follow sub commands if it is to make the ZyWALL exit sub command mode.

See Chapter 39 on page 499 for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

My packet capture captured less than I wanted or failed.

The packet capture screen’s **File Size** sets a maximum size limit for the total combined size of all the capture files on the ZyWALL, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The ZyWALL stops the capture and generates the capture file when either the capture files reach the **File Size** or the time period specified in the **Duration** field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the **File Suffix** field’s setting to avoid this.

44.1 Resetting the ZyWALL

If you cannot access the ZyWALL by any method, try restarting it by turning the power off and then on again. If you still cannot access the ZyWALL by any method or you forget the administrator password(s), you can reset the ZyWALL to its factory-default settings. Any configuration files or shell scripts that you saved on the ZyWALL should still be available afterwards.

Use the following procedure to reset the ZyWALL to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

If you want to reboot the device without changing the current configuration, see Chapter 42 on page 525.

1. Make sure the **SYS** LED is on and not blinking.
2. Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)
3. Release the **RESET** button, and wait for the ZyWALL to restart.

   You should be able to access the ZyWALL using the default settings.

44.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

A

Legal Information

Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications (Class B) ZyWALL 110 Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Certifications (Class A) ZyWALL 310, 1100 Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.

- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



"INFORMAZIONI AGLI UTENTI"

Ai sensi dell'art. 13 del Decreto Legislativo 25 luglio 2005, n.151

"Attuazione delle Direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti"

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

La raccolta differenziata della presente apparecchiatura giunta a fine vita è organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il

produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

ROHS

ENGLISH	DEUTSCH	ESPAÑOL	FRANÇAIS
Green Product Declaration RoHS Directive 2011/65/EU WEEE Directive 2002/96/EC (WEEE: Waste Electrical and Electronic Equipment) 2003/108/EC;2008/34/EC Declaration Signature: Name/Title: Raymond Huang / Quality & Customer Service Division/ Assistant VP. Date (yyyy/mm/dd): 2013/02/01	**Grünes Produkt Erklärung** RoHS Richtlinie 2011/65/EU ElektroG Richtlinie 2002/96/EG (ElektroG: Über Elektro- und Elektronik-Altgeräte) 2003/108/EG;2008/34/EG Unterschrift des Erklärenden: Name/Title: Raymond Huang / Quality & Customer Service Division / Assistant VP. Date (yyyy/mm/dd): 2013/02/01	**Declaración de Producto Ecológico** Directiva RoHS 2011/65/UE Directiva RAEE 2002/96/CE (RAEE : Residuos de Aparatos Eléctricos y Electrónicos) 2003/108/CE;2008/34/CE Firma de declaración: Nombre/Título: Raymond Huang / Quality & Customer Service Division / Assistant VP. Fecha (aaaa/mm/dd): 2013/02/01	**Déclaration de Produit Vert** Directive RoHS 2011/65/UE Directive DEEE 2002/96/CE (DEEE : déchets d'équipements électriques et électroniques) 2003/108/CE;2008/34/CE Signature de la déclaration : Nom/Titre : Raymond Huang / Quality & Customer Service Division / Assistant VP. Date (aaaa/mm/jj) : 2013/02/01
ITALIANO	**NEDERLANDS**	**SVENSKA**	
Prodotto dichiarazione di verde Direttiva RoHS 2011/65/UE Direttiva RAEE 2002/96/CE (RAEE: Rifiuti di Apparecchiature Elettriche ed Elettroniche) 2003/108/CE;2008/34/CE Firma dichiarazione: Nome/titolo: Raymond Huang / Quality & Customer Service Division / Assistant VP. Data (aaaa/mm/gg): 2013/02/01	**Productmilieuverklaring** RoHS Richtlijn 2011/65/EU AEEA-Richtlijn 2002/96/EG (AEEA: Afgedankte Elektrische en Elektronische apparatuur) 2003/108/EG;2008/34/EG Verklaringshandtekening: Naam/titel: Raymond Huang / Quality & Customer Service Division / Assistant VP. Datum(jjjj/mm/dd): 2013/02/01	**Miljödeklaration** RoHS Direktiv 2011/65/EU WEEE Direktiv 2002/96/EG (WEEE: om avfall som utgörs av eller innehåller elektriska eller elektroniska produkter) 2003/108/EG;2008/34/EG Deklaration undertecknad av: Namn/Titel: Raymond Huang / Quality & Customer Service Division / Assistant VP. Datum (åååå/mm/dd): 2013/02/01	

Index

Symbols

Numbers

3322 Dynamic DNS 215
3DES 306
3G see also cellular 132
6in4 tunneling 140
6to4 tunneling 141

A

AAA
  Base DN 402
  Bind DN 403, 405
  directory structure 402
  Distinguished Name, see DN
  DN 402, 403, 405
  password 405
  port 404, 407
  search time limit 405
  SSL 405
AAA server 400
  AD 402
  and users 372
  directory service 400
  LDAP 400, 402
  local user database 401
  RADIUS 400, 402, 406
  RADIUS group 406
  see also RADIUS
access 20
Access Point Name, see APN
access users 371, 373
  custom page 461
  forcing login 254
  idle timeout 379
  logging in 254
  multiple logins 380
  see also users 371
  Web Configurator 381
access users, see also force user authentication policies
account
  user 371, 438
accounting server 400
Active Directory, see AD
active protocol 310
  AH 310
  and encapsulation 311
  ESP 310
active sessions 72, 75, 89
AD 400, 402, 403, 405
  directory structure 402
  Distinguished Name, see DN
  password 405
  port 404, 407
  search time limit 405
  SSL 405
address groups 384
  and firewall 257
  and FTP 479
  and SNMP 483
  and SSH 475
  and Telnet 477
  and WWW 461
address objects 384
  and firewall 257
  and FTP 479
  and NAT 195, 224
  and policy routes 194
  and SNMP 483
  and SSH 475
  and Telnet 477
  and VPN connections 285
  and WWW 461
  HOST 384
  RANGE 384
  SUBNET 384
  types of 384

address record 452
admin user
troubleshooting 533
admin users 371
multiple logins 379
see also users 371
Advanced Encryption Standard, see AES
AES 306
AF 197
AH 289, 310
and transport mode 311
alerts 490, 491, 493, 495, 496, 497
ALG 233, 238
and firewall 233, 235
and NAT 233, 235
and policy routes 235, 238
and trunks 238
FTP 233, 234
H.323 233, 234, 238
peer-to-peer calls 235
RTP 239
see also VoIP pass through 233
SIP 233, 234
APN 136
Application Layer Gateway, see ALG
ASAS (Authenex Strong Authentication System) 401
asymmetrical routes 268
allowing through the firewall 271
vs virtual interfaces 268
attacks
Denial of Service (DoS) 288
Authenex Strong Authentication System (ASAS) 401
authentication
in IPSec 290
LDAP/AD 402
server 400
authentication algorithms 209, 306
and active protocol 306
and routing protocols 209
MD5 209, 306
SHA1 306
text 209
Authentication Header, see AH
authentication method objects 409
and users 372
and WWW 460
create 410
example 409
authentication policy 253
exceptional services 255
authentication type 46, 431
Authentication, Authorization, Accounting servers, see AAA server
authorization server 400

B

backing up configuration files 501
bandwidth
egress 137, 146
ingress 137, 146
bandwidth limit
troubleshooting 529
bandwidth management
maximize bandwidth usage 198, 352, 353
Base DN 402
Bind DN 403, 405
bookmarks 332
boot module 506
bridge interfaces 104, 160
and virtual interfaces of members 160
basic characteristics 104
effect on routing table 160
member interfaces 160
virtual 170
bridges 159

C

CA
and certificates 414
CA (Certificate Authority), see certificates
capturing packets 512
card SIM 137
CEF (Common Event Format) 488, 495
cellular 132
APN 136
interfaces 104

signal quality 94, 95
SIM card 137
status 96
system 94, 95
troubleshooting 529
certificate
troubleshooting 533
Certificate Authority (CA)
see certificates
Certificate Revocation List (CRL) 414
vs OCSP 428
certificates 413
advantages of 414
and CA 414
and FTP 478
and HTTPS 457
and IKE SA 310
and SSH 474
and synchronization (device HA) 369
and VPN gateways 285
and WWW 459
certification path 414, 420, 426
expired 414
factory-default 414
file formats 414
fingerprints 421, 427
importing 417
in IPSec 298
not used for encryption 414
revoked 414
self-signed 414, 419
serial number 421, 426
storage space 417, 423
thumbprint algorithms 415
thumbprints 415
used for authentication 414
verifying fingerprints 415
certification requests 419
certifications 537
notices 537, 538
viewing 538
Challenge Handshake Authentication Protocol (CHAP) 431
CHAP (Challenge Handshake Authentication Protocol) 431
CHAP/PAP 431
CLI 20, 24
button 24
messages 24
popup window 24
Reference Guide 2
client 341
cluster ID 361
commands 20
sent by Web Configurator 24
Common Event Format (CEF) 488, 495
compression (stac) 431
computer names 120, 157, 169, 174, 348
configuration
information 510, 515
web-based SSL application example 433
configuration file
troubleshooting 534
configuration files 499
at restart 502
backing up 501
downloading 503
downloading with FTP 478
editing 499
how applied 500
lastgood.conf 502, 505
managing 501
startup-config.conf 505
startup-config-bad.conf 502
syntax 500
system-default.conf 505
uploading 505
uploading with FTP 478
use without restart 499
connection
troubleshooting 530
connection monitor (in SSL) 99
connectivity check 119, 131, 137, 146, 156, 169, 290
console port
speed 449
cookies 20
copyright 537
CPU usage 72, 74
current date/time 71, 445
and schedules 396
daylight savings 447
setting manually 448
time server 449
current user list 99
custom

access user page 461
login page 461

D

Data Encryption Standard, see DES
date 445
daylight savings 447
DDNS 215
backup mail exchanger 219
mail exchanger 219
service providers 215
troubleshooting 530
Dead Peer Detection, see DPD
default
firewall behavior 265
Default_L2TP_VPN_Connection 346
Default_L2TP_VPN_GW 346
Denial of Service (Dos) attacks 288
DES 306
device access
troubleshooting 527
device HA 359
active-passive mode 359, 361
cluster ID 361
copying configuration 359
device role 363
HA status 361
legacy mode 359
management access 359
management IP address 359
modes 359
monitored interfaces 362, 365
password 364
synchronization 359, 369
synchronization password 364
synchronization port number 364
virtual router 361
virtual router and management IP addresses 362
device High Availability see device HA 359
DHCP 173, 444
and DNS servers 174
and domain name 444
and interfaces 174
client list 77
pool 174
static DHCP 174
DHCP Unique IDentifier 107
DHCPv6 438
DHCP Unique IDentifier 107
DHCPv6 Request 438
diagnostics 510, 515
Diffie-Hellman key group 307
DiffServ 197
Digital Signature Algorithm public-key algorithm, see DSA
direct routes 190
directory 400
directory service 400
file structure 402
disclaimer 537
Distinguished Name (DN) 402, 403, 405
DN 402, 403, 405
DNS 450
address records 452
domain name forwarders 453
domain name to IP address 452
IP address to domain name 452
L2TP VPN 348
Mail eXchange (MX) records 454
pointer (PTR) records 452
DNS inbound LB 247
DNS servers 47, 450, 453
and interfaces 174
documentation
related 2
domain name 444
Domain Name System, see DNS
DPD 300
DSA 419
DSCP 191, 194, 355, 521
DUID 107
Dynamic Domain Name System, see DDNS
Dynamic Host Configuration Protocol, see DHCP.
dynamic peers in IPSec 288
DynDNS 215
DynDNS see also DDNS 215
Dynu 215

E

egress bandwidth 137, 146
e-mail
  daily statistics report 485
Encapsulating Security Payload, see ESP
encapsulation
  and active protocol 311
  IPSec 289
  transport mode 311
  tunnel mode 311
  VPN 311
encryption
  IPSec 289
  RSA 421
encryption algorithms 306
  3DES 306
  AES 306
  and active protocol 306
  DES 306
encryption method 431
end-point security
  multiple objects 254
enforcing policies in IPSec 289
ESP 289, 310
  and transport mode 311
Ethernet interfaces 104
  and OSPF 111
  and RIP 110
  and routing protocols 109
  basic characteristics 104
  virtual 170
exceptional services 255
extended authentication
  and VPN gateways 285
  IKE SA 310
ext-user
  troubleshooting 533

F

FCC interference statement 537
file extensions
  configuration files 499
  shell scripts 499
file manager 499
file sharing SSL application
  create 435
Firefox 20
firewall 265
  actions 273
  and address groups 257
  and address objects 257
  and ALG 233, 235
  and H.323 (ALG) 234
  and HTTP redirect 230
  and IPSec SA 267
  and IPSec VPN 532
  and logs 257, 273
  and NAT 269
  and schedules 257, 273, 354, 356
  and service groups 273
  and service objects 391
  and services 273
  and SIP (ALG) 234
  and user groups 273, 275
  and users 273, 275
  and VoIP pass through 235
  and zones 265, 271
  asymmetrical routes 268, 271
  global rules 267
  priority 271
  rule criteria 267
  see also to-ZyWALL firewall 265
  session limits 267, 273
  to-ZyWALL, see to-ZyWALL firewall
  triangle routes 268, 271
  troubleshooting 528
firmware
  and restart 505
  boot module, see boot module
  current version 71, 506
  getting updated 505
  uploading 505, 506
  uploading with FTP 478
firmware upload
  troubleshooting 535
flash usage 72
forcing login 254
FQDN 452
FTP 478
  additional signaling port 237
  ALG 233

and address groups 479
and address objects 479
and certificates 478
and zones 479
signaling port 237
with Transport Layer Security (TLS) 478
full tunnel mode 317, 321
Fully-Qualified Domain Name, see FQDN

G

Generic Routing Encapsulation, see GRE.
global SSL setting 322
user portal logo 323
GRE 175
GSM 137
Guide
CLI Reference 2
Quick Start 2

H

H.323 238
additional signaling port 237
ALG 233, 238
and firewall 234
and RTP 239
signaling port 237
HA status see device HA 361
HSDPA 137
HTTP
over SSL, see HTTPS
redirect to HTTPS 459
vs HTTPS 457
HTTP redirect 229
and firewall 230
and interfaces 232
and policy routes 230
packet flow 230
troubleshooting 530
HTTPS 456
and certificates 457
authenticating clients 457
avoiding warning messages 466
example 465
vs HTTP 457
with Internet Explorer 465
with Netscape Navigator 465
hub-and-spoke VPN, see VPN concentrator
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

ICMP 390
IEEE 802.1q VLAN
IEEE 802.1q. See VLAN.
IKE SA
aggressive mode 305, 308, 309
and certificates 310
and RADIUS 310
and to-ZyWALL firewall 531
authentication algorithms 306
content 308
Dead Peer Detection (DPD) 300
Diffie-Hellman key group 307
encryption algorithms 306
extended authentication 310
ID type 308
IP address, remote IPSec router 305
IP address, ZyXEL device 305
local identity 308
main mode 305, 308
NAT traversal 309
negotiation mode 305
password 310
peer identity 308
pre-shared key 307
proposal 306
see also VPN
user name 310
inbound LB algorithm
least connection 249
least load 249
weighted round robin 249
inbound load balancing 247
time to live 250
incoming bandwidth 137, 146
ingress bandwidth 137, 146
interface

status 72, 84, 85
troubleshooting 528
interfaces 103
and DNS servers 174
and HTTP redirect 232
and layer-3 virtualization 104
and NAT 224
and physical ports 104
and policy routes 194
and static routes 197
and VPN gateways 285
and zones 104
as DHCP relays 174
as DHCP servers 174, 444
backup, see trunks
bandwidth management 173, 183, 184
bridge, see also bridge interfaces.
cellular 104
DHCP clients 172
Ethernet, see also Ethernet interfaces.
gateway 173
general characteristics 103
IP address 172
metric 173
MTU 173
overlapping IP address and subnet mask 172
port groups, see also port groups.
PPPoE/PPTP, see also PPPoE/PPTP interfaces.
prerequisites 105
relationships between 105
static DHCP 174
subnet mask 172
trunks, see also trunks.
Tunnel, see also Tunnel interfaces.
types 104
virtual, see also virtual interfaces.
VLAN, see also VLAN interfaces.
Internet access
troubleshooting 527, 532
Internet Control Message Protocol, see ICMP
Internet Explorer 20
Internet Protocol Security, see IPSec
Internet Protocol version 6, see IPv6
IP policy routing, see policy routes
IP pool 321
IP protocols 390
and service objects 391
ICMP, see ICMP
TCP, see TCP
UDP, see UDP
IP static routes, see static routes
IP/MAC binding 241
exempt list 244
monitor 91
static DHCP 243
IPSec 281
active protocol 289
AH 289
and certificates 285
authentication 290
basic troubleshooting 531
certificates 298
connections 285
connectivity check 290
Default_L2TP_VPN_Connection 346
Default_L2TP_VPN_GW 346
encapsulation 289
encryption 289
ESP 289
established in two phases 283
L2TP VPN 345
local network 281
local policy 288
manual key 288
NetBIOS 288
peer 281
Perfect Forward Secrecy 290
PFS 290
phase 2 settings 289
policy enforcement 289
remote access 288
remote IPSec router 281
remote network 281
remote policy 289
replay detection 288
SA life time 289
SA monitor 97
SA see also IPSec SA 310
see also VPN
site-to-site with dynamic peer 288
static site-to-site 288
transport encapsulation 289
tunnel encapsulation 289
VPN gateway 285
IPSec SA
active protocol 310
and firewall 267, 532

and to-ZyWALL firewall 531
authentication algorithms 306
authentication key (manual keys) 312
destination NAT for inbound traffic 313
encapsulation 311
encryption algorithms 306
encryption key (manual keys) 312
local policy 310
manual keys 312
NAT for inbound traffic 312
NAT for outbound traffic 312
Perfect Forward Secrecy (PFS) 311
proposal 311
remote policy 310
search by name 98
search by policy 98
Security Parameter Index (SPI) (manual keys) 312
see also IPSec
see also VPN
source NAT for inbound traffic 313
source NAT for outbound traffic 313
status 97
transport mode 311
tunnel mode 311
when IKE SA is disconnected 310
IPSec VPN
troubleshooting 531
IPv6 106
addressing 106
link-local address 106
prefix 106
prefix delegation 107
prefix length 106
stateless autoconfiguration 107
IPv6 tunnelings
6in4 tunneling 140
6to4 tunneling 141
IPv6-in-IPv4 tunneling 140
ISP account
CHAP 431
CHAP/PAP 431
MPPE 431
MSCHAP 431
MSCHAP-V2 431
PAP 431
ISP accounts 429
and PPPoE/PPTP interfaces 126, 429
authentication type 431
encryption method 431
stac compression 431

J

Java
permissions 20
JavaScripts 20

K

key pairs 413

L

L2TP VPN 345
Default_L2TP_VPN_Connection 346
Default_L2TP_VPN_GW 346
DNS 348
IPSec configuration 345
policy routes 346
session monitor 99
WINS 348
lastgood.conf 502, 505
Layer 2 Tunneling Protocol Virtual Private Network, see L2TP VPN 345
LDAP 400
and users 372
Base DN 402
Bind DN 403, 405
directory 400
directory structure 402
Distinguished Name, see DN
DN 402, 403, 405
password 405
port 404, 407
search time limit 405
SSL 405
user attributes 382
least connection algorithm 249
least load algorithm 249
least load first load balancing 178
LED troubleshooting 527

Lightweight Directory Access Protocol, see LDAP
load balancing 177
algorithms 178, 182, 184
DNS inbound 247
least load first 178
round robin 179
see also trunks 177
session-oriented 178
spillover 180
weighted round robin 179
local user database 401
log
troubleshooting 534
log messages
categories 491, 493, 495, 496, 497
debugging 100
regular 100
types of 100
logged in users 78
login
custom page 461
SSL user 328
logo
troubleshooting 534
logo in SSL 323
logout
SSL user 333
Web Configurator 22
logs
and firewall 257, 273
e-mail profiles 487
e-mailing log messages 102, 490
formats 488
log consolidation 491
settings 487
syslog servers 487
system 487
types of 487

M

MAC address
and VLAN 147
Ethernet interface 115
range 71
management access
troubleshooting 534
management access and device HA 359
Management Information Base (MIB) 480
manual key IPSec 288
MD5 306
memory usage 72, 75
Message Digest 5, see MD5
messages
CLI 24
metrics, see reports
Microsoft
Challenge-Handshake Authentication Protocol (MSCHAP) 431
Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) 431
Point-to-Point Encryption (MPPE) 431
model name 71
monitor 99
SA 97
monitored interfaces 362
device HA 365
mounting
wall 39
MPPE (Microsoft Point-to-Point Encryption) 431
MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) 431
MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) 431
MTU 137, 146
My Certificates, see also certificates 416

N

NAT 197, 221
ALG, see ALG
and address objects 195
and address objects (HOST) 224
and ALG 233, 235
and firewall 269
and interfaces 224
and policy routes 188, 195
and to-ZyWALL firewall 225
and VoIP pass through 235
and VPN 309
loopback 225
port forwarding, see NAT

port translation, see NAT
traversal 309
NBNS 120, 157, 169, 174, 321
NetBIOS
Broadcast over IPSec 288
Name Server, see NBNS.
NetBIOS Name Server, see NBNS
NetMeeting 238
see also H.323
Netscape Navigator 20
network access mode 18
full tunnel 317
Network Address Translation, see NAT
network list, see SSL 322
Network Time Protocol (NTP) 448
No-IP 215
NSSA 202

O

objects 318
AAA server 400
addresses and address groups 384
authentication method 409
certificates 413
schedules 396
services and service groups 390
SSL application 432
users, user groups 371, 438
One-Time Password (OTP) 401
Online Certificate Status Protocol (OCSP) 428
vs CRL 428
Open Shortest Path First, see OSPF
OSPF 201
and Ethernet interfaces 111
and RIP 203
and static routes 203
and to-ZyWALL firewall 201
area 0 202
areas, see OSPF areas
authentication method 111
autonomous system (AS) 201
backbone 202
configuration steps 204
direction 111
link cost 111
priority 111
redistribute 203
redistribute type (cost) 205
routers, see OSPF routers
virtual links 203
vs RIP 199, 201
OSPF areas 201, 202
and Ethernet interfaces 111
backbone 201
Not So Stubby Area (NSSA) 202
stub areas 202
types of 201
OSPF routers 202
area border (ABR) 202
autonomous system boundary (ASBR) 203
backbone (BR) 203
backup designated (BDR) 203
designated (DR) 203
internal (IR) 202
link state advertisements
priority 203
types of 202
other documentation 2
OTP (One-Time Password) 401
outgoing bandwidth 137, 146

P

packet
statistics 80, 81
packet capture 512
files 511, 514, 516
troubleshooting 535
packet captures
downloading files 511, 515, 516, 517
PAP (Password Authentication Protocol) 431
Password Authentication Protocol (PAP) 431
Peanut Hull 215
Peer-to-peer (P2P)
calls 235
Perfect Forward Secrecy (PFS) 290
Diffie-Hellman key group 311
Personal Identification Number code, see PIN code
PFS (Perfect Forward Secrecy) 290, 311
physical ports
packet statistics 80, 81

PIN code 137
PIN generator 401
pointer record 452
Point-to-Point Protocol over Ethernet, see PPPoE.
Point-to-Point Tunneling Protocol, see PPTP
policy enforcement in IPSec 289
policy route
  troubleshooting 528
policy routes 188
  actions 189
  and address objects 194
  and ALG 235, 238
  and HTTP redirect 230
  and interfaces 194
  and NAT 188
  and schedules 194, 354, 356
  and service objects 391
  and trunks 177, 194
  and user groups 193, 354, 356
  and users 193, 354, 356
  and VoIP pass through 235
  and VPN connections 194, 531
  benefits 188
  criteria 189
  L2TP VPN 346
  overriding direct routes 190
pop-up windows 20
port forwarding, see NAT
port groups 104
port roles 108
  and Ethernet interfaces 108
  and physical ports 108
port translation, see NAT
power off 526
PPP 175
  troubleshooting 529
PPP interfaces
  subnet mask 172
PPPoE 175
  and RADIUS 175
  TCP port 1723 175
PPPoE/PPTP interfaces 104, 125
  and ISP accounts 126, 429
  basic characteristics 104
  gateway 126
  subnet mask 126
PPTP 175
  and GRE 175
  as VPN 175
prefix delegation 107
problems 527
product registration 538
proxy servers 229
  web, see web proxy servers
PTR record 452
Public-Key Infrastructure (PKI) 414
public-private key pairs 413

Q

QoS 188, 349
Quick Start Guide 2

R

RADIUS 400, 402
  advantages 400
  and IKE SA 310
  and PPPoE 175
  and users 372
  user attributes 383
RADIUS server
  troubleshooting 532
RDP 432
Real-time Transport Protocol, see RTP
RealVNC 432
reboot 525
  vs reset 525
Reference Guide, CLI 2
registration
  product 538
related documentation 2
Relative Distinguished Name (RDN) 402, 403, 405
remote access IPSec 288
Remote Authentication Dial-In User Service, see RADIUS
remote desktop connections 432
Remote Desktop Protocol
  see RDP
remote management

FTP, see FTP
see also service control 456
Telnet 476
to-ZyWALL firewall 266
WWW, see WWW
remote network 281
remote user screen links 432
replay detection 288
reports
collecting data 87
daily 485
daily e-mail 485
specifications 89
traffic statistics 86
reset 535
vs reboot 525
RESET button 535
RFC
1058 (RIP) 199
1389 (RIP) 199
1587 (OSPF areas) 202
1631 (NAT) 197
1889 (RTP) 239
2131 (DHCP) 173
2132 (DHCP) 173
2328 (OSPF) 201
2402 (AH) 289, 310
2406 (ESP) 289, 310
2516 (PPPoE) 175
2637 (PPTP) 175
2890 (GRE) 175
3261 (SIP) 238
RIP 199
and Ethernet interfaces 110
and OSPF 200
and static routes 200
and to-ZyWALL firewall 200
authentication 200
direction 111
redistribute 200
RIP-2 broadcasting methods 111
versions 111
vs OSPF 199
Rivest, Shamir and Adleman public-key algorithm (RSA) 419
round robin 179
routing
troubleshooting 530
Routing Information Protocol, see RIP
routing protocols 199
and authentication algorithms 209
and Ethernet interfaces 109
RSA 419, 421, 427
RTP 239
see also ALG 239

S

schedule
troubleshooting 533
schedules 396
and current date/time 396
and firewall 257, 273, 354, 356
and policy routes 194, 354, 356
one-time 396
recurring 396
types of 396
screen resolution 20
SecuExtender 341
Secure Hash Algorithm, see SHA1
Secure Socket Layer, see SSL
security associations, see IPSec
security settings
troubleshooting 528
serial number 71
service control 456
and to-ZyWALL firewall 456
and users 456
limitations 456
timeouts 456
service groups 391
and firewall 273
service objects 390
and firewall 391
and IP protocols 391
and policy routes 391
services 390
and firewall 273
Session Initiation Protocol, see SIP
session limits 267, 273
session monitor (L2TP VPN) 99
sessions 89
sessions usage 72, 75

SHA1 306
shell script
troubleshooting 534
shell scripts 499
and users 383
downloading 508
editing 507
how applied 500
managing 507
syntax 500
uploading 509
shutdown 526
signal quality 94, 95
SIM card 137
Simple Network Management Protocol, see SNMP
Simple Traversal of UDP through NAT, see STUN
SIP 234, 238
ALG 233
and firewall 234
and RTP 239
media inactivity timeout 237
signaling inactivity timeout 237
signaling port 237
SNAT 197
troubleshooting 530
SNMP 479, 480
agents 480
and address groups 483
and address objects 483
and zones 483
Get 480
GetNext 480
Manager 480
managers 480
MIB 480
network components 480
Set 480
Trap 480
traps 481
versions 479
Source Network Address Translation, see SNAT
spillover (for load balancing) 180
SSH 472
and address groups 475
and address objects 475
and certificates 474
and zones 475
client requirements 474
encryption methods 474
for secure Telnet 475
how connection is established 473
versions 474
with Linux 476
with Microsoft Windows 475
SSL 317, 321, 456
access policy 317
and AAA 405
and AD 405
and LDAP 405
certificates 328
client 341
client virtual desktop logo 323
computer names 321
connection monitor 99
full tunnel mode 321
global setting 322
IP pool 321
network list 322
remote user login 328
remote user logout 333
SecuExtender 341
see also SSL VPN 317
troubleshooting 532
user application screens 333
user file sharing 334
user screen bookmarks 332
user screens 327, 331
user screens access methods 327
user screens certificates 328
user screens login 328
user screens logout 333
user screens required information 328
user screens system requirements 327
WINS 321
SSL application object 432
file sharing application 435
remote user screen links 432
summary 434
types 432
web-based 432, 435
web-based example 433
SSL policy
add 319
edit 319
objects used 318
SSL VPN 317
access policy 317

full tunnel mode 317
network access mode 18
remote desktop connections 432
see also SSL 317
troubleshooting 532
weblink 433
stac compression 431
startup-config.conf 505
and synchronization (device HA) 369
if errors 502
missing at restart 502
present at restart 502
startup-config-bad.conf 502
static DHCP 243
static routes 188
and interfaces 197
and OSPF 203
and RIP 200
metric 197
statistics
daily e-mail report 485
traffic 86
status 69
stub area 202
STUN 234
and ALG 234
supported browsers 20
synchronization 359
information synchronized 369
password 364
port number 364
restrictions 369
syslog 488, 495
syslog servers, see also logs
system log, see logs
system name 71, 444
system reports, see reports
system uptime 71
system-default.conf 505

T

TCP 390
connections 390
port numbers 390
Telnet 476
and address groups 477
and address objects 477
and zones 477
with SSH 475
throughput rate
troubleshooting 534
TightVNC 432
time 445
time servers (default) 448
token 401
to-ZyWALL firewall 266
and NAT 225
and NAT traversal (VPN) 531
and OSPF 201
and remote management 266
and RIP 200
and service control 456
and VPN 531
global rules 266
see also firewall 265
traffic statistics 86
Transmission Control Protocol, see TCP
transport encapsulation 289
Transport Layer Security (TLS) 478
triangle routes 268
allowing through the firewall 271
vs virtual interfaces 268
Triple Data Encryption Standard, see 3DES
troubleshooting 510, 515, 527
admin user 533
bandwidth limit 529
cellular 529
certificate 533
configuration file 534
connection resets 530
DDNS 530
device access 527
ext-user 533
firewall 528
firmware upload 535
HTTP redirect 530
interface 528
Internet access 527, 532
IPSec VPN 531
LEDs 527
logo 534
logs 534

management access 534
packet capture 535
policy route 528
PPP 529
RADIUS server 532
routing 530
schedules 533
security settings 528
shell scripts 534
SNAT 530
SSL 532
SSL VPN 532
throughput rate 534
VLAN 529
VPN 532
zipped files 529
trunks 104, 177
and ALG 238
and policy routes 177, 194
member interface mode 183, 184
member interfaces 183, 184
see also load balancing 177
Trusted Certificates, see also certificates 423
tunnel encapsulation 289
Tunnel interfaces 104

U

UDP 390
messages 390
port numbers 390
UltraVNC 432
upgrading
firmware 505
uploading
configuration files 505
firmware 505
shell scripts 507
usage
CPU 72, 74
flash 72
memory 72, 75
onboard flash 72
sessions 72, 75
user authentication 371
external 372
local user database 401
user awareness 373
User Datagram Protocol, see UDP
user group objects 371, 438
user groups 371, 372, 438
and firewall 273, 275
and policy routes 193, 354, 356
user name
rules 374
user objects 371, 438
user portal
links 432
logo 323
see SSL user screens 327, 331
user sessions, see sessions
user SSL screens 327, 331
access methods 327
bookmarks 332
certificates 328
login 328
logout 333
required information 328
system requirements 327
user-aware 258
users 371, 438
access, see also access users
admin (type) 371
admin, see also admin users
and AAA servers 372
and authentication method objects 372
and firewall 273, 275
and LDAP 372
and policy routes 193, 354, 356
and RADIUS 372
and service control 456
and shell scripts 383
attributes for Ext-User 372
attributes for LDAP 382
attributes for RADIUS 383
attributes in AAA servers 382
currently logged in 71, 78
default lease time 379, 381
default reauthentication time 379, 381
default type for Ext-User 372
ext-group-user (type) 371
Ext-User (type) 372
ext-user (type) 371
groups, see user groups

Guest (type) 371
lease time 376
limited-admin (type) 371
lockout 380
reauthentication time 376
types of 371
user (type) 371
user names 374

V

Vantage Report (VRPT) 488, 495
virtual interfaces 104, 170
basic characteristics 104
not DHCP clients 172
types of 170
vs asymmetrical routes 268
vs triangle routes 268
Virtual Local Area Network, see VLAN.
Virtual Local Area Network. See VLAN.
Virtual Network Computing
see VNC
Virtual Private Network, see VPN
virtual router 361
VLAN 140, 147
advantages 148
and MAC address 147
ID 147
troubleshooting 529
VLAN interfaces 104, 148
and Ethernet interfaces 148, 529
basic characteristics 104
virtual 170
VoIP pass through 238
and firewall 235
and NAT 235
and policy routes 235
see also ALG 233
VPN 281
active protocol 310
and NAT 309
and the firewall 267
basic troubleshooting 531
hub-and-spoke, see VPN concentrator
IKE SA, see IKE SA
IPSec 281
IPSec SA
proposal 306
security associations (SA) 283
see also IKE SA
see also IPSec 281
see also IPSec SA
status 76
troubleshooting 532
VPN concentrator 301
advantages 301
and IPSec SA policy enforcement 303
disadvantages 301
VPN connections
and address objects 285
and policy routes 194, 531
VPN gateways
and certificates 285
and extended authentication 285
and interfaces 285
and to-ZyWALL firewall 531
VRPT (Vantage Report) 488, 495

W

wall-mounting 39
warranty 538
note 538
Web Configurator 19
access 20
access users 381
requirements 20
supported browsers 20
web proxy servers 230
see also HTTP redirect
web-based SSL application 432
configuration example 433
create 435
weblink 433
weighted round robin (for load balancing) 179
weighted round robin algorithm 249
Windows Internet Naming Service, see WINS
Windows Internet Naming Service, see WINS.
Windows Remote Desktop 432
WINS 120, 157, 169, 174, 321
in L2TP VPN 348

WINS server 120, 348
Wizard Setup 33, 43
WWW 457
  and address groups 461
  and address objects 461
  and authentication method objects 460
  and certificates 459
  and zones 461
  see also HTTP, HTTPS 457

Z

zipped files
  troubleshooting 529
zones 211
  and firewall 265, 271
  and FTP 479
  and interfaces 211
  and SNMP 483
  and SSH 475
  and Telnet 477
  and VPN 211
  and WWW 461
  extra-zone traffic 212
  inter-zone traffic 212
  intra-zone traffic 212
  types of traffic 211